

SD Times

SOFTWARE DEVELOPMENT

The Industry Newspaper for Software Development Managers

SPECIAL REPORT

Slipping In
The Side Door
With
App Security
Message



page 23

AUGUST 15, 2006 • ISSUE NO. 156

www.sdtimes.com • \$7.95

The Fuzz: To Serve And Protect

Metasploit's browser bug hunt shows future of software testing

BY P.J. CONNOLLY

"Fuzzing"—or "fuzz testing"—is the practice of testing software by throwing random data at it. From a software security perspective, the goal is fault identification, whether the result is a buffer overflow, service denial, string injection or another problem.

Armed with a variety of so-called "fuzzers," H.D. Moore's Metasploit Project (www.metasploit.com) may have shown developers and testers that automated bug-hunting tools are the best way available to harden their code. Although Moore intended the recent "Month of Browser Bugs" to publicize what he characterized as the dangers of inadequate client-side browser security, one industry analyst finds it a needed wake-up call for developers of every stripe.

Moore, a co-founder of the Digital Defense risk assessment shop and the Open Source Vulnerability Project, and director of security research for Breaking-Point Systems, began July's so-called MoBB as a way to promote his blog, "Browser Fun" (browserfun.blogspot.com), which he dedicated to the topic of Web browser security research and vulnerability disclosure. After

► continued on page 8

Mercury Acquisition Leaves Testing, QA Tools in Limbo



CEO Mark Hurd wants to make software a 'crown jewel' of HP.

BY ALEX HANDY

When Hewlett-Packard announced late last month that it would be acquiring software tools vendor Mercury Interactive, the US\$4.5 billion price tag seemed to indicate a large investment into the IT management and governance space by the company Fortune magazine ranked as the 11th largest in the world. Indeed, HP made it clear that its OpenView products will benefit from the additional capabilities brought to the company by Mer-

cury's diverse product line, but little was said about Mercury's 10,000-plus quality assurance customers.

Mark Hurd, CEO of HP, in a conference call on the day the acquisition was announced, said, "We think this is a big opportunity for us and a big opportunity to make software truly a crown jewel of HP." Even HP's competitor, CA, agrees that the acquisition makes sense, but that doesn't mean industry analysts expect

► continued on page 12

SOA ADOPTION BRISK, VARIES BY INDUSTRY

BY EDWARD J. CORREIA

For most companies, the adoption of a service-oriented architecture is not a matter of if, but when. "SOAs rush into early adoption is remarkable," concluded Aberdeen Group, which published a study in June showing that 90 percent of companies around the world will have some SOA experience by the end of this year.

But take that with a grain of salt. The report, titled "Enterprise Service Bus and SOA Middleware," was paid for by Fiorano, IBM and TIBCO, all of which have dogs in the SOA hunt. Other studies, including Evans Data's Spring 2006 Web Services Development Survey, show more modest adoption rates but with a sharp increase in recent months. A Gartner report published in November indicates that adoption varies significantly by industry.

Of the nearly 400 U.S.-based developers and managers polled by Evans Data this spring, about one in four said they currently implement an SOA, an 85 percent increase from last year's survey. Aberdeen's was a global poll; about half of respondents were from the United States and a quarter from Europe.

Regardless of whose numbers paint a more lifelike picture, most would agree that SOA standards and technologies—SOAP, XML, UDDI, WS-* and others—have not only proven wor-

► continued on page 13

Xen and the Art of Virtualization

Microsoft joins industry heavyweights in backing project

BY ALEX HANDY

The Xen virtualization platform is fast gaining industry support, thanks to the contributions of companies such as HP, IBM, Novell, Sun and even Microsoft. During the month of July, IBM and HP both announced the introduction of support offerings for Xen running under SUSE, and Microsoft announced that it would begin working with Xen Source, the enterprise software company based on Xen, to foster better compatibility for the virtualization platform.

At the core of the HP and IBM announcements was the release of SUSE Linux 10. Novell's latest iteration of its Linux-based operating system now includes Xen as



SD Times Photo Illustration: Mara Leonardi

a standard part of both server and desktop installations. Since both HP and IBM are offering service and support contracts for their systems that run SUSE, both companies are also offering sup-

port for Xen. Interestingly, Microsoft will also be offering support for the tool when it releases Windows Server Longhorn.

But that doesn't mean that all

► continued on page 19

IN THIS ISSUE

At Sun, Two CTOs Are Better Than One3
Scaling Agile Practices for the Enterprise5
Instant Gratification in Help Department6
TestNG Reduces Confusion Over Results11
EclipseWorld Focuses on Callisto18
Wind River Linux Ready for Real Time20



Forget Time-to-Market;
It's About Time-to-Money page 26

HOLUB: The Next Big Thing27
BINSTOCK: Java EE? Yawn!28
O'BRIEN: New Looks at Books29
RUBINSTEIN: A 12-Step Program30



New Visual Studio 2005. The difference is obvious.

Spot the difference? You and all the members of your team will. Visual Studio® 2005 has new Team System lifecycle tools that get your team on the same page and working in sync. Plus, over 400 new features streamline coding, so you can focus on the work that matters. Spot the 10 differences above and play the game at msdn.microsoft.com/difference.

Microsoft
Visual Studio 2005

At Sun, Two CTOs Are Better Than One

First job is to get a handle on what company is doing; life-cycle tools a possibility

BY ALEX HANDY

Sun Microsystems' two CTOs have only been on the job since the summer began, but they already have a cohesive vision and goal: to tear down the silos. Tim Marsland and Bob Brewin share the position, and they both fully acknowledge that Sun's largest weakness is its scattered approach to business and development.

"We have to get a better idea, though this is embarrassing to admit, of exactly what we're doing," said Marsland, who was CTO of the Solaris product line before taking on the management of all Sun's systems software. "For the last several years we haven't really known what we're doing globally. We really want to be able to get a clearer idea on what our actual investment portfolio looks like and



Sun's two CTOs, Bob Brewin (left) and Tim Marsland, share the task of pointing the companies' products in the right direction.

where we're taking it." That, said Marsland, means looking over the current crop of software and systems offerings at Sun, and choosing projects that bring the best return on development investment.



Currently, both Marsland and Brewin feel that Solaris and NetBeans are the top horses in the race, though other possible areas of investigation include life-cycle management and server-based

video-on-demand solutions.

To coordinate the company's efforts better, Marsland and Brewin have divided up their duties. Said Marsland: "I'm more responsible for the systems-level software: the operating system. Bob is more focused on the application platform. There is some deliberate overlap. Obviously the idea of splitting the job up comes from the fact that it's such a big job. So far it's working out really well."

Brewin, who was formerly a distinguished engineer in Sun's developer tools organization, said that the many departments inside Sun have not traditionally worked together to integrate their products to the extent that other companies have. After only three weeks on the job, Brewin said that his goal was to foster increased communica-

tion and coordination among Sun's many internal developers and designers.

One way he hopes to accomplish this is by focusing more on the entire life cycle of software development, and to offer a cohesive management stack for developers working from start to finish. Brewin added that he will consider any possible software that could help fill in the gaps of Sun's life-cycle plays.

HEAVY LOSSES

But despite the candor of both Marsland and Brewin, Sun's beleaguered software business has yet to turn the corner. While the company's director of systems software marketing, Chris Rattcliffe, said that the company has been successfully selling its software as service and support contracts for more than a year now, Sun still took a heavy loss in Q4.

In late July, Sun announced that it took a US\$301 million loss for the fourth quarter of its 2006 financial year. On the bright side, the company saw its revenues increase by almost \$900 million over Q4 2005, but this included sales and licensing agreements of SeeBeyond, the \$200 million storage technology company Sun acquired two days before the end of the quarter.

But for now, the two men have their work cut out for them. Brewin is working with the team bringing Java into the open-source community, but declined to impart any new information on the process, preferring to repeat CEO Jonathan Schwartz's JavaOne statement: "It's not when we open-source Java, but how." ■

GPL 3.0 Revision Offers Patent Protection

New clause written by FSF offers covenant for users, developers

BY ALEX HANDY

A July revision of the controversial Free Software Foundation's GNU General Public License 3.0 draft adds a covenant to protect users of patented GPL software from legal action.

The prior draft of the license had drawn ire because of its unclear language in regard to patented GPL software.

Eben Moglen, general counsel of the FSF and co-author of the license, said, "We've spent a lot of time listening to a lot of people. We've done a good deal of redrafting and responding to ideas developed in the course of the spring."

Moglen included, with the second draft, an audio recording in which he explains the reasoning behind some of the changes in this draft. Among those reasons, he cited the expansion of digital rights management and the danger of GPL software being used as bait for patent lawsuits as two of the primary concerns addressed in this new draft.

"You certainly wouldn't want someone suing a user of free software for patent infringement. We want to make sure that nobody turns a patent or a patent license into a way of making a program that is free in

appearance un-free in reality," said Moglen in an interview with SD Times.

The newly added patent covenant appears in the completely revised section 11 of the second GPL 3.0 draft. In this section, the GPL reads, "You receive the Program with a covenant from each author and conveyor of the Program, and of any material, conveyed under this License, on which the Program is based, that the covenanting party will not assert (or cause others to assert) any of the party's essential patent claims in the material that the party conveyed, against you, arising from your exercise of rights under this License."

Essentially, said Moglen, this new paragraph means that the rights granted in the GPL cannot be suspended by a software patent. But, Moglen added, this does not mean that software licensed under the GPL cannot be patented: If a developer patents software that's licensed under GPL 3.0, the developer cannot then mandate that end users have a patent license in order to modify said program.

The revised patent section closes out with a newly added clarification that ensures soft-

ware patents and copyright privileges that do not infringe upon the GPL's protections are fair game. "Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law."

But the softened and clarified take on patents doesn't mean that the Free Software Foundation thinks that software patents are a good idea. "The FSF is a very realistic foundation. Mr. Stallman and his colleagues have always been clear that there's only so much you can do [about

patents in the GPL]. The patent problem hurts everybody because it's a bad way to think about software, to think of it as patentable," said Moglen. Richard Stallman is the founder and chairman of the FSF.

Other revisions to the GPL 3.0 include a mandate that requires that all additional licensing information added to software licensed under the GPL be included in the source code. The new draft also broadened the definition of what it means to make source code publicly available to include sharing over peer-to-peer networks. ■

3D DESKTOP

Novell last month began shipping SUSE Linux Enterprise 10, which includes updated versions of its SUSE Linux Enterprise Server and Enterprise Desktop distributions. The desktop edition includes an Xgl-based GUI with tiling and 3D effects, pictured, and integrated versions of OpenOffice.org 2.0 and Beagle search. New in the server edition is AppArmor application-level security, Xen virtualization, ZENworks management and new storage components that Novell says let the server run Oracle's Real Application Clusters straight out of the box. Pricing for version 10 has been reduced and simplified from prior editions.



Register Online Today!

The industry's independent conference for enterprise software developers and IT development managers using Eclipse tools and technologies

At EclipseWorld, you will...

- Learn how to save money and improve developer productivity with Eclipse
- Improve team collaboration using Eclipse-based tool sets.
- Go beyond the IDE to understand the wide range of Eclipse technologies.
- Get deep inside Eclipse's open-source architecture.
- Discover the best, most effective Eclipse add-ins and plug-ins.
- Learn how to build better applications using the Eclipse RCP.

The Eclipse Foundation is proud to host the annual EclipseWorld conference. The 2005 EclipseWorld in New York City is a must-attend event for enterprise IT professionals. The Eclipse community has embraced the

"Well organized and enjoyed the presentations."

Alice Chan, Software Engineer, Cytoscape

"Good sessions on the basics as well as plug-ins."

Patricia Terrie, Senior Software Engineer

Are you ready for Eclipse?

...an Eclipse master, ...started with the platform, ...decide if Eclipse technologies

eclipse

WORLD

The Enterprise Development Conference

Hyatt Regency Cambridge
Boston, MA
September 6-8

There's Still Time!
Register Now!
www.eclipseworld.net

EclipseWorld had a great collaborative atmosphere. It was exciting to learn about current uses of Eclipse, and see what others are creating with it."

Justin Strom, Software Engineer, Auspice

...being discussed in the ...was very leading edge. ...familiarize myself with projects ...a chance to research."

James Pitt, Director of Database Programming, Embarcadero Technologies

Keynote Speaker

...director of the ...he has held key man- ...WebGain, The Object ...y International Inc. (which ...olly owned subsidiary of ...ability for development, ...marketing, strategic planning, ...ss development.



Mike Milinkovich,
Executive Director,
Eclipse Foundation

A BZ Media Event

BZ Media is an Associate Member of the Eclipse Foundation.

Diamond Sponsor

COMPUWARE
www.compuware.com



Platinum Sponsor

SYBASE

Gold Sponsors

openmake
a product of **total st**

PARASOFT
the maker software work

Silver Sponsors

instantiations

ACTUATE

GENWIRE

Media Sponsors

SDTimes

Software Test & Performance

ECLIPSE REVIEW

EclipseSource

queue

Software

eclipse

Methods & Tools

javareference

Extension MEDIA

For sponsorship or exhibiting information, contact
Donna Esposito at 415-785-3419 or desposito@bzmedia.com.

www.eclipseworld.net

Scaling Agile Practices for the Enterprise

Project management solutions deal with requirements, tool integrations

BY DAVID RUBINSTEIN

One of the issues that has held back adoption of agile development methodologies in large organizations, advocates acknowledge, is scalability. Two well-known vendors of agile project management software released products in late July to deal with the issue.

Rally Software released Rally Enterprise, life-cycle management software that features Agile Accelerators that offer prescriptive services to organizations regarding methods and tools. It also introduces traceability and versioning around requirements management.

Also last month, VersionOne released V1: Agile API, which lets customers tie into such life-cycle tools as bug trackers, IDEs and requirements management tools. "The API extends the natural progression from tool to product to platform," said VersionOne president and CEO Robert Holler. The API also extends V1: Agile Enterprise, a life-cycle management product released in April that is being updated with the ability to notify team members about requirements, features or tasks via RSS.

EXPOSED AS AN API

Holler explained that prior to the release of the Agile API, connections to life-cycle tools could be made manually, but now, he said, all the reads and writes are exposed as a Web service API.

Rally's Enterprise platform also offers portfolio management metrics through reporting and executive dashboards, which give the status of a life-cycle process, according to Mike Metcalf, Rally's vice president of marketing.

"Some teams have to justify their existence and need levels of metrics and reporting," said Ryan Martens, Rally's founder and CTO. "They need to show they're making progress on quality, efficiency and customer satisfaction, and these aren't even agile shops."

Martens also noted that in many enterprises, regulatory compliance is an issue that must be faced "without forcing them into a model that scales through longer planning cycles, upfront waste, and less emphasis on getting out quality software."

Metcalf said a feature of note

is that the platform is available as an on-demand service or with an on-premises installation.

Rally's service model delivers the project management

software as a VMware image, with charts and burndowns given in a rich-client, AJAX-like interface, Martens said.

The Agile Accelerators pro-

vide what Rally calls "maturity services," which at first help implement agile practices, then deal with requirements gathering from the product's owners,

and then help organizations tackle concurrent engineering and velocity increases. Its "scaling services" are designed to assist with multiteam project management and with blending agile practices into the entire organization, Metcalf explained.

Rally expects to ship the tools in mid-August. ■



Removes the hurdles between project planning and project implementation



DevPlan

Use DevPlan to define project deliverables

- Manage milestones, timelines, and resources
- Attach designs, specifications, and requirements to create a fully conceptualized product before development work begins
- Schedule events to co-ordinate resources, enforce deadlines, and drive deliverables



DevTrack

Use DevTrack to manage its implementation

- Manage implementation items, changes, features, defects, and project issues using an action-based workflow
- Track development work within the context of a project and associate work items to source code deliverables
- Run configurable reports that can be published dynamically to the web

TechExcel

www.techexcel.com | 1-800-439-7782

complete SOA testing platform

**It works,
it doesn't
work...**



**Is this how
you test SOA?**

Time to pick the most complete SOA testing solution on the market. Aptly named iTKO LISA 3 Complete SOA Test Platform.

Test continuously. From unit and functional tests, to regressions, to load and performance tuning, LISA covers your development lifecycle.

Test everything. LISA is a test client to every component, from the web app to middle-tier SOAP, Java and .NET, databases, EJBs and messaging.

Everyone tests. LISA's no-code testing allows developers, QA teams and business analysts to deeply test every layer of your SOA for errors and business rules, exactly as it will be delivered.

**Meet iTKO LISA 3,
and fall in love
with testing again.**

iTKO LISA

www.itko.com

Now There's Instant Help For Enterprise Applications

Zion Software blends instant messaging, AJAX

BY EDWARD J. CORREIA

Instant oatmeal, instant coffee, instant gratification...Americans like to have things now. Making that happen for software is Zion Software, which last month released Instant Help to enable IM-based application help systems across an enterprise or the Internet. It began shipping on July 18.

According to Zion CTO David Ferrero, Instant Help lets developers create buttons on a Web page that correspond to applications or assistance categories within an application. Take, for example, an HR application that does not allow employees to access their HR information through a browser. "The HR department might have a button [created] that employees can press to ask how many vacation days they have left," he said.

The button would initiate an AJAX-based IM session between the employee and the existing IM client of one or more designated HR people whose real screen names remain private. At times, buttons can be "grayed out" based on rules or staff availability. "This aggregates the presence information of multiple people in terms of that button. You could also set up times of day when that help is available," using an included rules engine, he added.

Instant Help works through a company's in-house IM system—Jabber, Lotus Sametime or Microsoft LCS—or with public IM systems such as AIM, Google Talk, MSN and Yahoo Messenger, or a combination. Also required is JBuddy Message Server, Zion's IM message and routing engine for Java SE 1.4 or higher, which costs US\$30 per user per month.

Available as a hosted service, Instant Help costs an additional \$30 per month per concurrent session plus a gateway for each IM network (Sametime, AIM, etc.) to be used. Gateways cost between \$1,000 and \$2,000 each. "If a company buys just

one concurrent help session, only one person can get instant help at a time. If a second person needs help at the same time, their questions go into a queue," he explained. The self-hosted version costs \$399 per concurrent session. SDKs, which include APIs and libraries, are available for Java, .NET and ColdFusion.

Ferrero said that Zion's licensing model is among its strongest competitive differentiators. LivePerson, Zion's main competitor, prices its LivePerson Contact Center based on the number of customer service rep (CSR) seats. "A company might have five or 10 CSRs, and you pay for each of those on a monthly basis," he said. Zion's model, he explained, is more like the phone company's. "You might have five or 10 phone lines that everyone in the company shares."

Instant Help also permits help sessions to be transferred to other users. "You can have three or four people on tech questions and transfer to an engineer for one-off technical questions," Ferrero said. LivePerson would require such escalations to use a backchannel with the specialist, he added, such as a phone call or separate IM session.

In the future, Zion might permit Instant Help buttons to be part of a desktop application's interface. "We contemplated putting buttons in various deployed enterprise applications so that users could click a button and request help from within the application," Ferrero said.

For now, front-end interfaces are built using AJAX and HTTP. "From an end user's perspective, they come to a Web site, click a button and get help," he said. Help reps also can be automations, or bots. "You could use the bot to grab articles based on certain keywords [in a query]." Bots count as concurrent help sessions. A bot SDK is under development. ■



Instant Help buttons can be created that correspond to help categories or a help desk.

Naturally Integrated.™



Chart FX for Visual Studio 2005

The Most Tightly Integrated Data Visualization Tool Available for Visual Studio 2005

Evidence of this is the **Smart Tag Wizard** that exposes many of the properties to select and display in real-time. There is also a **Data Wizard** which allows you to quickly connect to a data source, map specific fields to the chart and instruct the chart how to use the data. The **new API** was designed with the Visual Studio 2005 object model in mind to make it easier to access complex functionality. Chart FX for Visual Studio 2005 adds a **DHTML rendering engine** that uses the AJAX (Asynchronous JavaScript and XML) web development technique to produce chart images that allow full interactivity and support state in web applications. The new **Extensions Manager** standardizes the infrastructure for using the Chart FX Extensions, such as financial, statistical, maps and OLAP, among others. The Chart FX **Resource Center** provides a "Programmer's Guide", the Chart FX API, an Internet Reference and a wealth of samples and charts (with code). *Learn more about the seamless integration and powerful features at www.softwarefx.com.*


Chart FX
for Visual Studio® 2005

www.softwarefx.com

©2006 Software FX. All rights reserved. Chart FX is a registered trademark of Software FX, Inc. All other brands are owned by their respective owners.

News Briefs

NEW PRODUCTS

Middleware solutions developer Fiorano Software has released a native .NET runtime for its **ESB 2006** and **SOA 2006** platforms. The component adds support for C#, Visual Basic, Visual C++ and all of Microsoft's other .NET languages to existing native bindings for C, C++ and Java.

UPGRADES

Solid Information Technology in late July began beta testing **solidDB for MySQL**, a version of its high-performance transactional database storage engine for MySQL Server. It is available under the GPL ... Green Hills Software has unveiled **TraceEdge-PMC**, a version of its TimeMachine debugger for embedded systems that permits collection of trace data from PowerPC processors that do not have a trace port by diverting it through a PCI Mezzanine Card (PMC). The PMC edition joins other TraceEdge products that use real-time trace ports, standard PCI slots, target memory and local processor busses ... Adobe Systems has announced the availability of the **Flex 2** products for developers focused on rich Internet applications. The Flex 2 platform



includes the company's Flash Player runtime; Flex Builder, an Eclipse-based IDE; and Flex Data Services, a server-side J2EE application managing data delivery, paging and synchronization. The Flex 2 SDK and Flex Data Services 2 Express are free of charge; Flex Builder is available for US\$499, while Flex Data Services 2 is \$20,000 per CPU plus maintenance and support. Flex 2 Builder runs on Windows 2000 and XP, while Flex Data Services can support a variety of Linux, Unix and Windows server-class systems running appropriate application server software ... Version 2 of **Doc-To-Help 2006** was released by ComponentOne last month, in both the Enterprise and the Doc-To-Help for Word versions, which cost US\$999.95 and \$749.95, respectively. ComponentOne claims the new release offers users better command-line support, flexible linking and publishing options, improved developer support and (Rehabilitation Act of 1973) Section 508-compliant output. The Enterprise version adds natural search, support for HTML formats, and Microsoft FrontPage and Macromedia Dreamweaver integration to the basic "for Word" package. Doc-To-Help subscribers will receive the updated versions as part of their subscriptions; competitive upgrades are also available ... **Little G**, a lightweight version of the Geronimo application server, has been released in conjunction with **Apache Geronimo version 1.1**. The full-featured



Geronimo 1.1 adds a configuration and management console that provides access to the plug-in architecture of the server. It also boasts structural changes designed to improve scalability and organization ... On the heels of its acquisition of NetIQ, Attachmate in late July released version 6.0 of **Verastream Host Integrator**, its newly acquired screen-based host access solution, with several productivity enhancements. Among those are new debugging capabilities that reduce the time to diagnose and repair malfunctions.



Also new are the ability to copy objects to ease the creation of data designs and the ability to deploy and test those models without requiring a local production server. Verastream Host Integrator enables developers to capture data and logic with the screen interface for use in Web services or other components, such as COM, JavaBeans, .NET or XML ... SlickEdit has released **version 3.2** of its code editor plug-in for Eclipse, enabling developers to make the tool the default editor within any Eclipse-based IDE. The Eclipse platform went to version 3.2 in June, and this release keeps pace, according to the company. The editor includes such features as comment wrapping, the ability to specify tag jump orders and code templates. Available immediately, the plug-in costs US\$199 for new licenses and \$99 for licensees seeking an upgrade ... Windward Studios' **Windward Reports .NET Server Engine 4.1** allows developers using Microsoft's .NET platform to generate reports using Windward's Chart and Graph output formats, and for the first time the tool provides an XLS output. Windward introduced the .NET version of the reporting engine in January; previously, it was available only for Java. The engine uses J# and requires .NET 2.0, according to the company. ■

Metasploit's Browser Bug Hunt Shows Future of Software Testing

◀ continued from page 1

posting a bug for each day of the month, the lion's share of the bugs Moore turned up were in Internet Explorer—25, across both Windows XP and Windows 2000.

But Moore's been trying to break other browsers as well, and with some success. Apple's Safari, KDE's Konqueror, Mozilla's Firefox and Opera 9 all turned up on the MoBB hit list for one reason or another. Although Moore was careful to avoid posting exploit code in the MoBB listings, his tools gave him the details for the recipes that invoke each bug.

Four of the five tools Moore used to ferret out the browser flaws are publicly available through the Metasploit Project site; the last is under test, according to Moore. The "CSSDIE" tool focuses on pushing funky style values through CSS (Cascading Style Sheets), while "Hamachi" does the same with Dynamic HTML. A third tool adds and removes DOM (Document Object Model) elements to find problems with implementations of DHTML, and finally, "Mangle" creates what its author, Michal Zalewski, describes as "tiny, razor-sharp shards of malformed HTML" and feeds them to the browser under test to detect "NULL pointer references, memory corruption, buffer overflows and sometimes memory exhaustion."

MIXED REACTION

Vendor reaction to the MoBB revelations was mixed. When contacted, Apple and the Mozilla Foundation declined comment. In a similar vein, Microsoft's public response noted that serious bugs had been fixed in a recent security update, others merely crashed IE, and elsewhere noted that the company supported the practice of "responsible disclosure... directly to a vendor." Moore posted the Opera 9 bug as this article was being written: Opera Software reports the bug is fixed in the upcoming 9.01 release.

However, the KDE Project was willing to speak, with U.S. representative Ian Reinhart Geiser noting that the bug was



Moore's blog promotion demonstrated the need for browser 'fuzz testing.'

in its database, was expected to be fixed in the next release, and that the episode demonstrated a "powerful feature" of Metasploit's testing methods. Since open-source projects don't have the resources to trawl through every vulnerability list, he noted, KDE and similar projects relied on outside input and direct notification of bugs.

Forrester Research senior analyst Michael Gavin sees Moore's efforts and the Month of Browser Bugs, in particular, as excellent demonstrations of the usefulness of fuzzing tools in QA and security testing. From his perusal of the MoBB blog, he believes Moore has handled the situation responsibly. "He's not releasing code that allows you to exploit these things; he's giving proof-of-concept: 'Here's something interesting, and this is how we found it.'"

The important thing, Gavin said, is that developers, QA

and testers all need to understand that "they could be finding these kinds of things just as well as he can."

He went on to argue "a large percentage of security vulnerabilities would disappear if people tested for these types of things." Fuzzing, he said, is a good way to test for invalid input, which he claimed accounted for around 90 percent of known vulnerabilities.

When asked if Microsoft was living up to its pledge to make its software more secure, Gavin observed, "There's room for improvement." But he conceded that with the size of Microsoft's codebase, vulnerabilities are bound to turn up.

"The bigger lesson to be learned here is to take what [Moore's] doing and apply it to server-side code," he said, noting that while crashing a client-side browser is a nuisance, a compromised server application can be a catastrophe. ■

BROWSER BUG SCORECARD

Opera 9 (Windows)	1 bug
Memory corruption triggered by long URL, fixed in 9.01 release.	
Konqueror (KDE 3.5.1 on Gentoo Linux)	1 bug
Fix expected in next version.	
Safari 2.0.4 (Mac OS X 1.4.7)	2 bugs
DHTML flaw crashes browser, KHTML parser allows code execution.	
Mozilla 1.5 (Gentoo Linux, Windows 2000/XP)	2 bugs
JavaScript errors; 1 bug fixed in version 1.5.0.3, 1 bug fixed in version 1.5.0.5.	
Internet Explorer (Windows 2000/XP)	25 bugs
Latest IE on XP SP2: 19	
Latest IE on XP SP2 with Outlook/other Office components: 3	
Latest IE on Win2000 SP4: 3	
14 NULL dereference bugs, 4 invalid memory use bugs, 2 stack overflows and 5 miscellaneous flaws	

Source: browserfun.blogspot.com

The Switch is On

PKWARE® made the switch to Surround SCM™

Now it's your turn!



Tom Francis
Software Architect
PKWARE

Joe Sturonas
Chief Technology Officer
PKWARE

Switch Now for FREE!*



More and more development teams are switching to Seapine's Surround SCM. That's because Surround SCM makes the switch easy and **gives you more**. Surround SCM provides you with a richer set of source code management features and a more productive work environment than other tools. PKWARE switched from Microsoft® Visual SourceSafe® to Surround SCM because of Surround's rock-solid stability, collaboration capabilities, and usability features. Other companies are switching for the same reasons.

Competitive upgrade offer for VSS, CVS, and PVCS users!

For a limited time, Seapine is offering a FREE named user license when you switch from Microsoft® Visual SourceSafe®, CVS, or Merant/Intersolv PVCS® to our award-winning Surround SCM. Plus, once you're part of the Seapine family, you'll receive a number of unmatched benefits including Seapine's world-class *Customer Care*. Thousands of users have made the switch, and more are switching every day. Isn't it time you did and got more from your SCM tool?

Visit www.seapine.com/switch to get the full story on why PKWARE made the switch and how to take advantage of this special upgrade offer. Or, call **1-888-683-6456** to speak with a Seapine product specialist. Mention offer code UG003 to receive your free license.



Joe Sturonas
Chief Technology Officer
PKWARE

"PKWARE wanted a product that was flexible enough to support the multi-platform development we require as we move forward to create the next generation of data security products. VSS lacked the advanced functionality necessary for parallel code work. Surround SCM efficiently enables our collaborative development process."



Tom Francis
Software Architect
PKWARE

"Most software configuration management tools expect users to conform their processes to the tool, and usually involve IT support to implement. Surround SCM is sophisticated enough to work with our complex development environment, and Seapine's high level of responsiveness is impressive."

*Offer is valid for one named user license per company.

Visit <http://www.seapine.com/switch> for complete upgrade details and other licensing information.

©2006 Seapine Software, Inc. Seapine Surround SCM and the Seapine logo are trademarks of Seapine Software, Inc. All Rights Reserved. All other products mentioned are the property of their respective owners.

 **Seapine Software**™
Managing Process, Change & Quality
Throughout the Enterprise

Embarcadero Revs DB Design Tools

New ER/Studio adds model validation, data security tags, full session undo/redo

BY P.J. CONNOLLY

Embarcadero Technologies released ER/Studio 7.1, an update to its data architecture and database design tools, last

month. The new version supports Sybase IQ and a variety of DBMSes from Hitachi, IBM, Informix, InterBase, Microsoft, MySQL, NCR Teradata, Ora-

cle and Sybase. ER/Studio 7.1 also includes a new model validation wizard that recognizes both logical and physical models and offers more

than 50 tests to enforce consistency at an enterprise level. Another new feature intended to make modelers more productive is support for *n*-tier undo

and redo throughout a session. ER/Studio "makes it easier to look into a database, analyze the data that's there, and document that data," claimed Nancy Blum, Embarcadero's director of product marketing.

Blum noted that while many customers know they want to secure their data, they often ask, "How do I know what data to secure?" ER/Studio 7.1 attempts to address that question by introducing data properties that allow database designers and DBAs to tag data and objects by the level of sensitivity, a necessary step toward formalized data governance. She pointed out that although making services available may be a good thing, developers "have to understand [the nature of] the data they're using."

ER/Studio 7.1 runs on Windows and comes in a Standard "stand-alone" edition, or an Enterprise version that offers team collaboration features and Embarcadero's ER/Repository. ■



ActiveReports for .NET

Got Data? Show It!

New Version 3.0

- ✓ Annotations
- ✓ Enhanced Chart
- ✓ Visual Basic .NET Scripting
- ✓ Design-Time Support for .NET Data Providers





EASY to USE

ActiveReports features an easy-to-use, banded, fully integrated report designer with built-in wizards, integrated toolbars, report and field explorer window, print preview with bookmarks, text search and thumbnails, a full-featured chart control, and a detailed help file. With ActiveReports, it is easy to create the kinds of reports you need—from the most basic to the most complicated reports.

EASY to LICENSE

Licensing with ActiveReports for .NET is straightforward and easy to understand. There are no hidden costs, no extra licensing fees and no royalties charged for end users. Once you install the product after purchase, you are free to create and deploy your reports as needed.

EASY to DEPLOY

ActiveReports makes deploying your reports and end-user reporting capabilities easy. The reporting engine is provided as a single managed, strongnamed assembly. ActiveReports allows assemblies to be distributed using XCopy or placed in the Global Assembly Cache (GAC).

Standard Edition

\$599 per developer, royalty free

Professional Edition

\$1499 per developer, royalty free

ACT QUICKLY!

Upgrade discount for current users expires in January 2007

Optimized for



www.datadynamics.com

5870 Cleveland Avenue
Columbus, Ohio 43231
614-895-3142
Fax: 614-899-2943



Infragistics Unites AJAX, JSF

BY DAVID RUBINSTEIN

Looking to help developers who want to leverage both JavaScript and the Java platform, software component seller Infragistics last month released NetAdvantage for JSF 2006, a set of AJAX-enabled JavaServer Faces components for building user interfaces for J2EE applications.

"NetAdvantage for JSF shows what is possible with the combination of AJAX and JSF," said Tom Hammell, Infragistics' Java product manager, in a news release announcing the product. The components let users load large data files without the need for using post-backs, the company explained in the release.

The component set, which ships with support for Sun's Studio Creator development suite, includes grids, menus, trees and tabs. It can be used in applications running on major Java application servers, the company said.

NetAdvantage for JSF costs US\$795 on an annual subscription basis; with priority support, it costs \$1,290. ■

TestNG 5.0 Smoothes Out Annotations

Test tool update reduces confusion when running thousands of tests

BY ALEX HANDY

TestNG's ability to organize thousands of unit tests has improved with the release of version 5.0 in late July.

Cédric Beust, a software engineer at Google, explained that he began developing TestNG three years ago because he believed JUnit was too limited in scope for proper enterprise use. Beust acknowledged that JUnit is the more popular unit testing tool for Java, but that his own TestNG offers better options for handling large numbers of tests.

"The major feature [in this release] is not brand-new; it's about more renaming and cleanup of annotation names to make them more intuitive. Our reports are easier to read and better organized now. As we have more and more users who have thousands of tests and dozens of groups, it becomes really important to make those reports easy to read," said Beust, who is originally from France.

But despite being open-source, the project has remained primarily a two-man affair. Most of the third-party work has been done on making TestNG work with IDEs such as Eclipse, NetBeans and IntelliJ IDEA. But outside of those contributions, most of the work on the project has been done exclusively by Beust and Alexandru Popescu, who began contributing code soon after Beust created TestNG.

For the future, Beust would like to see more contributors to the TestNG project, but doesn't expect many changes to its core functionality. "For the past year, there were less features requested in the core, and we were working on productivity around

the core, which is good because it means the core is working and functional enough," said Beust of the 600-strong mailing list for the tool.

"I think we're going to see stronger integration with Web servers so we can drive TestNG from remote machines," Beust added, saying that he's also cre-

ating a version that can handle distributed tests. "The general message is going to be more about scaling. For people writing thousands of tests, we want

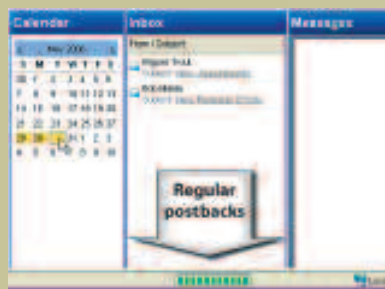
to make it almost transparent for them to use as many machines and as much power as they have."

Despite Beust's employment at Google, the tool has little to do with the company. TestNG is a free and open-source tool. It can be downloaded at www.testng.org. ■

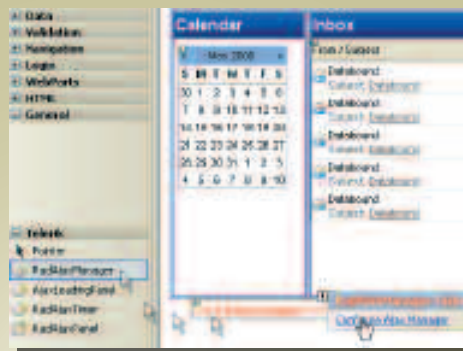
telerik
deliver more than expected

1min < AJAX-enable any application < 2 min

Reporting Solution



ASP.NET UI Suite



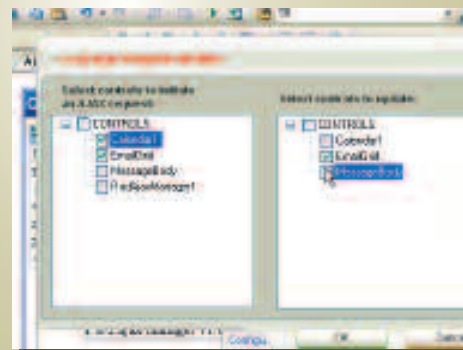
AJAX Framework

WinForms UI Suite



Step 1:
Drag the AJAX Manager control on the WebForm
Total time: ~ 5 sec.

Step 2:
Use the single dialog to set:
• which controls initiate AJAX
• which controls are updated with AJAX
Total time: < 1.55 min.



• No Previous AJAX Experience Needed

r.a.d.ajax does not require any prior experience with AJAX. You don't need to learn an "AJAX-specific" way of building new applications.

• No Modifications to Your Application Necessary

No need to place Callback Panels around areas that need to be updated. No need to set triggers or manually invoke AJAX requests.

• Intuitive and Centralized Management of AJAX Relations

All relations between controls which initiate AJAX and those that are updated with AJAX are managed from a single dialog.

• Codeless Development

Drag-and-drop the AJAX Manager control on the page, tick the respective checkboxes in the dialog, and hit F5.

See r.a.d.ajax demonstrated at these events:

AJAXWORLD
CONFERENCE & EXPO
(Santa Clara, CA Oct. 2-4)

FTP Online's
AJAX virtual tradeshow
(www.ftponline.com/virtual/ajax/)

Watch a video at:

www.telerik.com/ajaxvideos

GET THE SCOOP!

FREE E-Newsletter

Subscribe to SD Times' News on Monday and News on Thursday at

www.sdtimes.com

HP Acquisition Leaves Mercury Test Tools in Limbo

MERCURY'S LINEUP

Mercury's product lines are primarily split between management tools and QA tools. The company's numerous management tools track and control everything from software changes to time management to customer demands and compliance. These applications include:

Application Delivery Foundation	Demand Management	Program Management
Application Management	Deployment Management	Project Management
Administration	End User Management	Resource Management
Application Mapping	Financial Management	Service Desk
Business Availability Center	IT Governance Center	Service Level Management
Center Management	Performance Center	System Availability Management
Change Control Management	Portfolio Management	Time Management

The company's monitoring tools focus primarily on watching large-scale business Web sites and compliance with business process rules. Also, the company's Diagnostics and SiteScope tools offer QA for the field.

Client Monitor	Global Monitor
SiteScope	Diagnostics
Real User Monitor	Business Process Monitor

Mercury's Quality Center is the overarching QA tool suite that the company uses as the focal point of its testing infrastructure. The company's popular LoadRunner load-testing tool also comes in dozens of flavors specific to IBM DB2, Oracle and other common enterprise systems.

Quality Center	TestDirector
Business Process Testing	QuickTest Professional
Functional Testing	WinRunner
LoadRunner	

Can This Really Work?

HP's takeover history is rocky. Will things be different?

BY JENNIFER DEJONG

Can HP make the Mercury acquisition work?

Research analysts answered with a tentative "yes." They said Mercury's testing and application management tools align reasonably well with HP's OpenView network management offerings. But they were quick to point out HP's flawed record of integrating earlier acquisitions, and its lack of experience in the testing tools arena.

"HP has a rocky history with acquisitions," said ARM Research analyst Dennis Gaughan. "But I have higher hopes of success this time around."

Chief among the failed acquisitions cited is Compaq, which HP acquired in 2002 in a stock swap deal worth an estimated US\$25 billion. "There were a lot of teething problems integrating the various groups," noted Bola Rotibi, an analyst for U.K.-based Ovum. And when HP's former CEO, Carly Fiorina, stepped down last year, failure to make the Compaq merger work was widely perceived as a key reason, said Rotibi. "There is some fear that could be replicated with Mercury."

Less high-profile, but also flawed, was the Bluestone Software acquisition. HP bought the Java application server maker for an estimated \$500 million



Carly Fiorina was at the helm when HP bought Compaq and Bluestone.

in 2001. Initially, HP positioned the Bluestone application server as a stand-alone offering, said Jim Jackson, who works for HP's technology solutions group. But in 2004, HP forged a partnership with JBoss, pledging its support for the open-source application server.

The thinking behind the Bluestone acquisition was completely unclear, said Carey Schwaber, an analyst at Cambridge, Mass.-based Forrester Research. "But I don't think there is as much opportunity to do badly with Mercury."

The market for application servers was still emerging when HP bought Bluestone, but that's not the case with Mercury, she said. "It is a mature company, and the market for

testing tools is mature."

More troubling is HP's lack of experience in the testing tool arena. "When you look at what HP is saying, they are not talking about testing," said Schwaber. In making the announcement, HP articulated its vision for integrating its OpenView network management offerings with Mercury's tools for application management, she said.

"Testing was given only the most cursory mention [by HP]," echoed Ovum's Rotibi. But Mercury derives 60 percent of its revenue from QA tools, she said. "At the end of the day, they are a testing company." And HP has no background in the testing world, she said.

Integrating network management and application management tools still leaves some holes, Schwaber said. "It will still treat actual development as a black box, and that is a problem."

A key reason why IDC analyst Stephen Elliot remains optimistic about the deal is Mark Hurd, who took the helm as HP's CEO and president in March 2005.

"Hurd brings a new perspective on what it means to integrate an acquisition," he said. "With Hurd there is a back to basics [mentality], a focus on market share and customers." ■

◀ continued from page 1

the acquisition to be an easy touchdown.

Carey Schwaber, an analyst at Forrester Research, said the acquisition "definitely raises some new challenges" for HP. "It's a new market for HP. They've not been in testing before. They have made some moves into the application development space, and they've ended badly."

But, despite HP's spotty acquisition track record, Schwaber does not expect the company to ignore Mercury's testing customers. "Considering the number [of customers], which is more than 10,000, HP will definitely be very careful to do no harm. I don't anticipate any real change for [those customers], other than a very pointed introduction to the rest of the HP software portfolio. Mercury had been pitching its systems management capabilities to these customers already, so they're kind of a soft target at this point," added Schwaber.

On the SOA side of the fence, the Mercury acquisition finally brings Systinet's offerings into the HP family. According to Jason Bloomberg, senior analyst at ZapThink, HP bid for Systinet earlier this year. Mercury ultimately won that bidding war, however, and Bloomberg believes that the Mercury acquisition was somewhat influenced by the fact that HP still had designs on the Systinet repository and other SOA tools.

"HP has been strong in SOA for a while, and Mercury has as well, especially since they acquired Systinet," said Bloomberg. "By putting HP OpenView in the initiative, there's a clear story these sides are telling."

HERE COMES THE JUDGE

For Mercury, the acquisition has a distinct benefit: It puts to rest many of the investment and bookkeeping controversies that have plagued the company for the past two years.

Last year, the company was forced to restate its earnings for 2002, 2003 and 2004, due to the alleged back-dating of stock options given to employees. Even HP's Hurd acknowledged that these issues could be addressed in the eventual purchase agreement, possibly through reserves held back from the purchase price pending the

refiling of earnings reports.

But Bloomberg believes that Mercury's legal troubles are actually being solved by this acquisition. "Once the acquisition is closed, there'll be no more company called Mercury," said Bloomberg. "It's a shortcut out of trouble."

Schwaber said that HP had originally put in a bid for Mercury six months ago, but that the final price tag was significantly higher than the original bid. This, said Schwaber, was an indication that rival storage company EMC had started a bidding war for the company.

CA CTO Al Nugent said that the purchase was a good one for HP, but added that the acquisition does leave some holes that need to be filled if HP wants to compete in the IT management space. "I think what HP has discovered is there's a lot more to end-to-end IT management than being able to provide the network and provide the service desk. There's more to it than managing a network and managing an application," he said.

"You would continue to compare what CA is doing to what HP is doing," said ZapThink's Bloomberg. "They've both been through some management changes. They've both been through some of the SEC problems," he said.

"At this point, it looks like CA is slightly ahead because they've completed their acquisitions," said Bloomberg, adding that, for HP, "there may be some things missing, but there's fewer pieces missing than before."

HP's Hurd claimed the acquisition is a perfect fit, citing the near-total lack of overlap between the companies' product lines. He hinted that the initial integration period will be marked by significant cost-cutting. And that, said Schwaber, will be a great indication of how the acquisition is going.

"We'll want to look at who stays at Mercury with HP," said Schwaber. "A lot of people at Mercury grew up at Mercury, so staff turnover will be a big deal. We want to look at whether HP provides technology support at the rate Mercury did. [Mercury] had amazing environment support." Added Schwaber: "Mercury wasn't the most thrifty company, so there's a little bit of [cost-cutting] opportunity." ■

SOA Adoption Brisk, Varies by Industry

◀ continued from page 1

thy as a means to reuse components within an organization, but have also enabled Web services to become a worldwide infrastructure foundation.

John Andrews, president of Evans Data, attributes the jump in adoption to an increase in education. "People are learning the advantages of SOA in technology and in the business side," he said. "There's no question that SOA is beneficial. This allows companies to extend resources to fund these efforts."

Aberdeen characterizes SOA as "a major technology wave driven by the unbearable costs of technology integration, which is programmer labor-intensive." By breaking applications into component services, SOA simplifies the line-of-business process changes mandated by management, Aberdeen says, causing IT to embrace SOA as a "long-term cost reducer and tool to accelerate time-to-market."

But according to Andrews, companies will need to spend significantly before they begin to realize those cost savings.

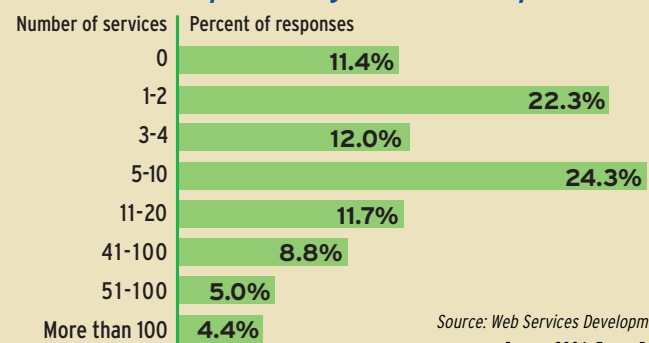
"Companies have been struggling with the upfront investment it takes to implement an SOA architecture," he said. "The whole emphasis is on code and component reuse. Until you get to that stage, it costs more and takes more time," he said.

In the past, Andrews said, when companies put a project together to solve a business need, they were solving the problem for a single-business audience. "Now you're looking at how to take advantage of reusability across as many services as possible. It's a more complete design process upfront," and complex in terms of implementation, he added. "In time, though, you'll have that reusability, so it should pay for itself."

SOA SILOS

With the expense and resource drain involved in SOA implementation, the results of Gartner's industry study showing banking, insurance, investment and health-care industries as top adopters might on the surface seem quite logical.

What is the current number of production Web services in your IT organization this year?



Beyond financial, the reasons cited in the November report for the high adoption rates of those industries might not be so obvious.

In banking, Gartner reported the highest adoption rates at 78 percent. Competition is fierce, and banks, regardless of size, must respond quickly to changes in "market and customer demands, channel offerings and shifts in competitor strategies," the Gartner report stated.

Insurance companies, on the other hand, have used SOA as a way to deploy functionality of their vintage applications to

agents and brokers via the Web. As a result, Gartner said, insurance companies have changed the way they store claim and policyholder information and the way claims, policies and customers relate to one another.

Such a structure could be thought of in terms of ERP SOA, one of three deployment types that Aberdeen's research identified. ERP SOA deployments, in place in about one-sixth of responding companies, are defined as a preferred integration method into applications and as a low-cost SOA toolkit for integration of ERP data out to

other applications or processes, as in the insurance industry.

The other two methods, SOA Lite and Enterprise SOA, occupy opposite ends of the deployment spectrum. Aberdeen found that the SOA Lite category is dominated by small-to-mid-size companies and users of Microsoft .NET technologies. SOA Lite is predominantly focused on Web services that are not mission-critical and "do not require high-volume scalability, high availability and failover, management, governance and security." Enterprise SOA deployments do require all those capabilities, and are generally synonymous with companies with annual revenue of at least US\$1 billion per year.

Other significant hurdles remain, Andrews said, including security and testing. "Because you have to do integration testing across architectures, finding issues also is a major inhibitor when IT is already being accused of being too slow to react to business needs. But over time, it will expedite reusability." ■

Get More

Surround SCM gives you more advanced source code management and version control capabilities than competitive products.

- **Powerful productivity tools** such as advanced branching, Guiffy compare/merge, automated triggers, and more.
- **Team-based collaboration and communication** including automatic change notifications, detailed change history, and flexible repository options.
- **Seamless integration** with TestTrack™ Pro and a wide variety of development and build tools.
- **Scalable, cross-platform client/server support** for team deployment on Windows®, Solaris®, Linux®, and Mac® OS X®.
- **Low cost of ownership** means easy to install, use, and maintain. No administration is required.

Accelerate your development effort today! Download your FREE fully functional evaluation software now at www.seapine.com/sdtsscsm or call 1-888-683-6456.



Switch Now for FREE!

For a limited time, Seapine is offering a FREE named user license when you switch from Microsoft® Visual SourceSafe®, CVS, or Merant/Intersolv PVCS® to our award-winning Surround SCM. Thousands of users have made the switch, and more are switching every day. Isn't it time you did and got more from your SCM tool?

PKWARE Made the Switch to Surround SCM. Now it's Your Turn!

Visit www.seapine.com/switch to get the full story on why PKWARE made the switch and find out how to take advantage of this special upgrade offer. Mention offer code UG003 to get your FREE named user license.

*Offer is valid for one named user license per company.

JS-Sorcerer Has Command Line in Its Power

BY ALEX HANDY

Vi and Emacs users can now benefit from the capabilities of JS-Sorcerer, the JavaScript development tool from DHI Technologies, which works not only within Eclipse but also

from a command line.

JS-Sorcerer is a US\$199-per-user tool that offers syntax checking, variable type and flow analysis, and type-safe linking for external files to JavaScript developers.

Among the many new features of JS-Sorcerer 2.0 are additional file integration capabilities that allow developers to seamlessly combine HTML and JavaScript files into singular cohesive wholes. Also added in

this version is a dependency generator that tracks the requirements inside of JavaScript files, and functions that help manage JavaScript libraries and the order in which they load.

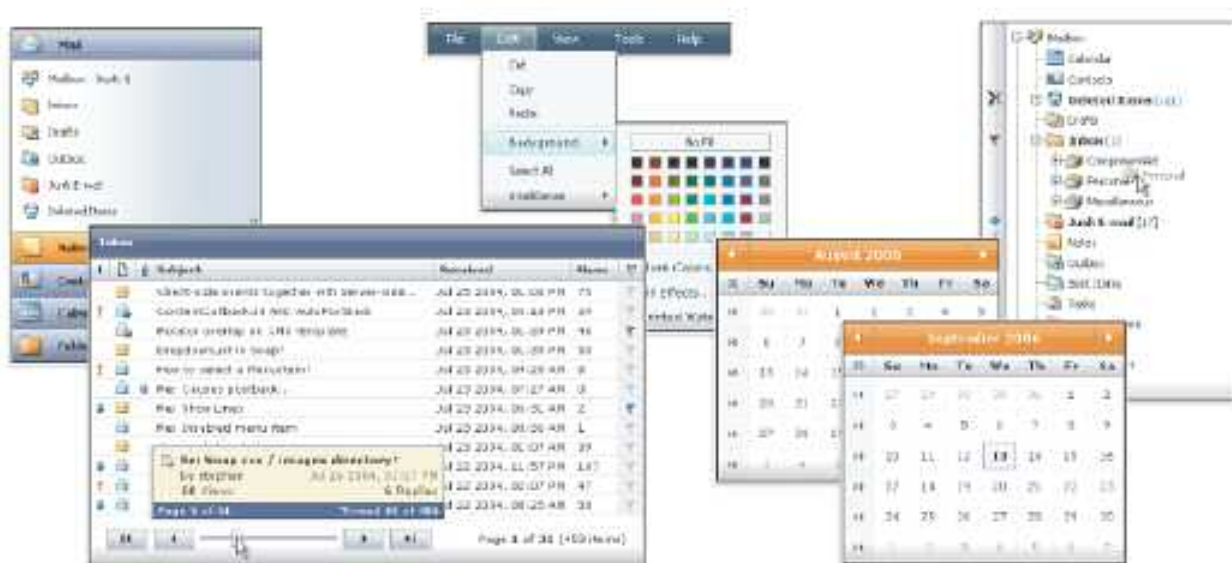
"We believe that the initial

investment of several days to learn JS-Sorcerer, and to modify the structure of legacy applications, is quickly returned by the long-term benefit it offers to serious Web application developers," said Roger Franklin, CEO of DHI.

JS-Sorcerer 2.0, like its earlier incarnations, also functions as an Eclipse plug-in, though this version supports the Web Tools Platform as well. JS-Sorcerer 2.0 runs under Linux, Mac OS X and Windows. A 15-day free trial can be downloaded at www.dhitechnologies.com. ■

Web User Interfaces, evolved.

The most advanced set of AJAX enabled UI controls for ASP.NET



ComponentArt

Web.UI 2006.1

for ASP.NET

Try Web.UI 2006.1 today at www.componentart.com

Web.UI 2006.1 combines ComponentArt's outstanding rendering technology with the power of AJAX to deliver the richest set of user interface controls available for ASP.NET. Version 2006.1 adds two new controls - Spinner and WebChart Lite - and introduces an unsurpassed level of client-side programmatic control, along with extensive ASP.NET 2.0 support.

ComponentArt
www.componentart.com

ATALASOFT: PUT AJAX ON THAT IMAGE

BY ALAN ZEICHICK

The newest version of Atalasoft's .NET imaging toolkit, DotImage, focuses on improving the interactivity of ASP.NET applications by adding new AJAX features, according to the company, and also has new capabilities for automatically cleaning scanned images and applying photographic effects.

DotImage 4.0, which shipped at the end of July, now has an AJAX-based thumbnail control that lets end users view and process Web-based images without postbacks, according to the company.

The latest release also adds new component modules for advanced document cleanup and advanced photo effects. The cleanup module removes specks, borders, broken or dotted lines, holes and other unwanted elements from scanned or other images being processed by the application. The photo effects module, designed for high-end photography and prepress applications, can be used to apply color corrections, boost shadows, or improve the appearance of skin tones in photographs.

The DotImage component suite, which works with both .NET 1.1 and .NET 2.0 assemblies, is available in two versions. For photo processing, the cost is US\$499 per developer seat, plus \$329 for each production deployment server. For document imaging, DotImage costs \$1,799 per developer seat, plus \$999 for the production deployment server. ■

Functional Testing Converges With Consulting Service

BY ALEX HANDY

Convergys has introduced an automated testing tool that aims to place test design in the hands of novice users. Easy Test is designed to build functional tests through a point-and-click interface. The tool also supports keyword-, table- and data-driven tests, which can be built in a plain language-based scripting engine.

According to Andrea Ayers, the company's president of government and new markets, Convergys built Easy Test to address needs that were unmet by commercially available products. "After client requests to make this solution commercially available, we created Convergys Testing Solutions, including the Convergys Easy Test application testing tool," she said.

The company uses its software tools heavily in its consulting services. According to Jean Hervé Jenn, Convergys' president of international operations, tools are only one of the many solutions his company offers, as is evidenced by Convergys' work with German television company Unity and its subsidiary, Arena.

"Working with Unity and Arena enabled us to apply our

operational expertise and proven software products to configure and implement a solution that meets their particular billing and customer care requirements and aggressive

implementation timeline," said Jenn.

Easy Test runs on Windows and costs US\$12,000 per user. It is a stand-alone testing suite that can be used even before

work on a piece of software is complete. Testers are also given the ability to step through errors found in an application without the need to stop a test and start over once a bug has been found.

Convergys said that its tool, released in late June, is primarily aimed at organizations that are seeking to expand internal testing by placing unskilled testers on QA projects. ■

Web Service For Data Storage

BY P.J. CONNOLLY

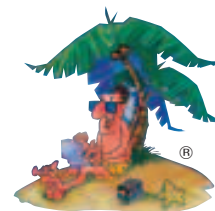
Online digital media service provider Streamload made a move last month toward the enterprise market by launching its eponymous Web service, targeted at developers and content providers who require secure and reliable data storage and online services.

Streamload Web Services consists of two components, the first being the free-for-use Streamload Platform API, which allows developers to access and build on the features of MediaMax, the company's online media center.

The second part of the Web service is Streamload Storage and Processing Services, focusing on the needs of digital media consumers and developers for large amounts of online storage, rapid media transcoding, and broad-scale file transfer without the customer incurring big costs. ■

Your best source for software development tools!

programmer's paradise®



LEADTOOLS Raster Imaging Pro for .NET by LEAD Technologies

Extend and simplify the .NET framework and GDI+ with LEADTOOLS. Support for over 140+ file formats including TIFF, JPG, J2K*, PDF*, and GIF using various compression schemes like JPEG, JPEG2000, LZW, CCITT G3/G4, and CMP. Scan, capture, 200+ image processing filters, high speed display (resize, rotate, quality controls), and much more. Lots of sample source code to get you started quickly!

*Requires plug-in

Paradise # L05 053R
\$829.99

www.programmers.com/lead



c-tree Plus® by FairCom

With unparalleled performance and sophistication, c-tree Plus gives developers absolute control over their data management needs. Commercial developers use c-tree Plus for a wide variety of embedded, vertical market, and enterprise-wide database applications. Use any one or a combination of our flexible APIs including low-level and ISAM C APIs, simplified C and C++ database APIs, SQL, ODBC, or JDBC. c-tree Plus can be used to develop single-user and multi-user non-server applications or client-side application for FairCom's robust database server—the c-treeSQL™ Server. Windows to Mac to Unix all in one package.

Paradise # F01 0131
\$850.99

www.programmers.com/faircom



AllFusion® ERwin® Data Modeler r7 Plus 1 Year Enterprise Maintenance by CA

Introducing AllFusion® ERwin® Data Modeler r7, rising to the challenge of successful information management starts with optimal database design. Enables visualization of complex data structures, inventory information assets and establishes enterprise-wide standards for managing data. Automates the design process and synchronizes the model with the database design. Use this product to design transactional systems, data marts and data warehouses in one integrated environment. Enhanced "out of the box" support for Oracle 10g/9i.

Paradise # P26 03SD
\$3687.99

www.programmers.com/ca



WebWorks ePublisher Pro for Word by Quadralay

Online Help Power Tool

Easily deliver professional content for six different online Help systems, plus eight standard online formats. Efficient XML-based processing and an intuitive workflow streamline content production for the Web, cross-platform online Help, portable devices, and PDFs.

Paradise # W21 015B
\$893.99

www.programmers.com/webworks

dtSearch Web with Spider

Quickly publish a large amount of data to a Web site

- Dozens of full-text and fielded data search options.
- Highlights hits in XML, HTML and PDF, while displaying links and images; converts other files ("Office," ZIP, etc.) to HTML with highlighted hits.
- Spider adds local or remote web sites (static and dynamic content) to searchable database
- Optional API supports SQL, C++, Java, and all .NET languages.

Download dtSearch Desktop with Spider for immediate evaluation

Single Server
Paradise # D29 0726
\$888.99

"Bottom line: dtSearch manages a terabyte of text in a single index and returns results in less than a second." —InfoWorld

www.programmers.com/dtsearch

TX Text Control 12.0

Word Processing Components

TX Text Control is royalty-free, robust and powerful word processing software in reusable component form.

- .NET WinForms control for VB.NET and C#
- ActiveX for VB6, Delphi, VBScript/HTML, ASP
- File formats RTF, DOC, HTML, XML, TXT
- PDF export without additional 3rd party tools or printer drivers
- Nested tables, headers & footers, text frames, bullets, numbered lists, multiple undo/redo
- Ready-to-use toolbars and dialog boxes

Professional Edition
Paradise # T79 0218
\$739.99

Download a demo today.

www.programmers.com/theimagingsource

Xtreme ToolkitPro 2006

by CodeJock Software

Xtreme ToolkitPro 2006 provides the most comprehensive set of fully customizable user interface components for the development of Microsoft® style applications for use with Microsoft Foundation Class (MFC) and Microsoft .NET development platforms.

Newer Features include:

- SkinFramework Control
- Report Control
- Calendar Custom Print
- Calendar Reminders
- Office 2007 Style Ribbon Control
- Calendar Multi-Schedule Support
- MS Outlook 2003*, MySQL and SQL Server compatibility for Xtreme Calendar.



Paradise # CBC 004R
\$566.99

www.programmers.com/codejock

Multi-Edit 2006

by Multi Edit Software

Speed, depth, uncompromising program access. Multi-Edit 2006 provides a great tool for your programming arsenal. Search with definable filters & Perl 5 Regular Expression support.

BCDiff by Scooter Software enhances ME's file comparing. Other features are integration with ImageMagic, Delphi 2006, C++ Builder 2006, Visual Studio 2005 and code beautifying support for 15 languages. Handle over 50 languages including Ruby.



Paradise # A30 016W
\$211.99

Upgrade A30 016Y
\$126.99

www.programmers.com/multiedit

Paradise Picks



DevTrack 6.0 Powerful Defect and Project Tracking by TechExcel

DevTrack, the market-leading defect and project tracking solution, comprehensively manages and automates your software development processes. DevTrack features sophisticated workflow and process automation, seamless source code control integration with VSS, Perforce and ClearCase, robust searching, and built-in reports and analysis. Intuitive administration and integration reduces the cost of deployment and maintenance.

www.programmers.com/techexcel

Paradise # T34 0206
\$482.99



/n software Red Carpet Subscriptions by /n software

/n software Red Carpet™ Subscriptions give you everything in one package: communications components for every major Internet protocol, SSL and SSH security, S/MIME encryption, Digital Certificates, Credit Card Processing, ZIP compression, Instant Messaging, and even e-business (EDI) transactions. .NET, Java, COM, C++, Delphi, everything is included, together with per developer licensing, free quarterly update CDs and free upgrades during the subscription term.

www.programmers.com/nsoftware

Paradise # D77 0148
\$1444.99

800-445-7899

Prices subject to change. Not responsible for typographical errors.

www.programmers.com

"Best concentration of

Announcing The Third Annual

Software Test & Performance CONFERENCE



November 7-9, 2006

**The Hyatt Regency
Cambridge, MA**

The Software Test & Performance Conference provides technical education for test/QA managers, software developers, software development managers and senior testers.

The wall between test and development has fallen, and the Software Test & Performance Conference brings the whole application life cycle together!

BUT DON'T TAKE OUR WORD FOR IT...

"This is the best conference I have attended. The instructors were extremely knowledgeable and helped me look at testing in a new way."

—Ann Schwerin, QA Analyst
Sunrise Senior Living

**For Sponsorship and
Exhibitor Information
Contact David Karp at
631-421-4158 x102 or
dkarp@bzmedia.com**

Diamond Sponsor



Platinum Sponsors



Gold Sponsors



Silver Sponsor



Media Sponsors



"If you get one impact idea from a conference it pays for itself. I got several at the

performance testing presentation/professionals I've seen." — Nathan White, Manager, Testing Services, AG Edwards

- **OPTIMIZE** Your Web Testing Strategies
- **LEARN** How to Apply Proven Software Test Methodologies
- **NETWORK** With Other Test/QA & Development Professionals
- **ACHIEVE** a Better Return on Investment From Your Test Teams
- **GET** the Highest Performance From Your Deployed Applications

"This is a conference to help both testers and developers as well as managers and leads. There is enough variety and content for everybody."

—Michael Farrugia, Software Engineer
Air Malta

"Great topics – well presented by reputable presenters. Having attended two years in a row, I have yet to be disappointed."

—Arden Sharp, QA Manager
SunGard

"Excellent conference – provided a wide range of topics for a variety of experience levels. It provided tools and techniques that I could apply when I got back, as well as many additional sources of information."

—Carol Rusch, Systems Analyst
Associated Bank

"This conference is great for developers, their managers, as well as business-side people."

—Steve Margenau, Systems Analyst
Great Lakes Educational Loan Services

"I've received volumes of new information and ideas to share with my team."

—Theresa Harmon, Business
Applications Developer
Pharmacare Specialty Pharmacy

"Reputable speakers and presenters. Great class topics."

—Jung Manson, QA Manager
Webloyalty.com

"Very informative and a good chance to network with others."

—Marty P... Technical ...ant
Autodesk

"A conference with something for everyone."

— Scott L. Boudreau, QA Manager, Tribune Interactive



**Register by
SEPT. 15 to take
advantage of the
Super Early
Bird Rates!**

**REGISTRATION
IS NOW OPEN**
www.stpcon.com

STP Conference." — Patrick Higgins, Senior Software Test Engineer, SSAI

EclipseWorld 2006 Focuses on Callisto

BY EDWARD J. CORREIA

Web Tools, the Rich Client Platform and the Eclipse Test & Performance Tools Platform are new tracks at EclipseWorld 2006, taking place Sept. 6-8 in Boston. There are also several

classes and a tutorial dedicated to Callisto, the most recent releases of the Eclipse IDE and related projects.

One of this year's most popular technical classes, based on early registration information

from organizer BZ Media, which publishes SD Times and the monthly Eclipse Review magazine, appears to be "Building Commercial-Quality Plugins for Eclipse," from Eric Clayberg and Dan Rubel,

authors of a popular book of the same name.

The conference keynote will be delivered by Mike Milinkovich, executive director of the Eclipse Foundation, on Thursday, Sept. 7. ■

Advanced Digital Dashboards require Advanced Data Visualization





Dundas

Data Visualization

Create powerful Digital Dashboards using Advanced Data Visualization solutions from Dundas!

Dundas Chart, Dundas Gauge and Dundas Diagram offer the latest award-winning technologies that Fortune 500 companies across the globe trust to create advanced Dashboard applications.

Being the leader in Data Visualization solutions for the .NET framework, Dundas' products are all designed to give organizations the tools they need to dynamically visualize all their Key Performance Indicators (KPI's) and other critical data in real time.

With built-in data analysis and sophisticated visual customization abilities, Dundas' solutions offer a comprehensive feature set for the quick creation of advanced Digital Dashboards.

To download a full evaluation copy of any of Dundas' line of Data Visualization Solutions, visit www.dundas.com.

Dundas
Chart
for .NET

Dundas
Gauge
for .NET

Dundas
Diagram
for .NET

www.dundas.com

Featuring
Microsoft
Visual Studio .NET
Technology

Microsoft, Visual Studio, Visual Studio.NET are registered trademarks of Microsoft Corporation in the United States and/or other countries

www.dundas.com
info@dundas.com
(416) 467-5100
(800) 463-1492

Advanced Data Visualization for Microsoft® Technologies



CONFERENCE: Sept. 6-8
Hyatt Regency Cambridge, Boston

TUTORIALS:
Wednesday, 8:45 am-5:00 pm

CLASSES:
Thursday, 8:30 am-4:45 pm
Friday, 8:30 am-5:00 pm

EXHIBIT HOURS:
Thursday, 2:45 pm-7:30 pm
Friday, 12:00 pm-4:00 pm

KEYNOTE:
Thursday, 5:00 pm-5:45 pm,
Mike Milinkovich, Eclipse Foundation
www.eclipseworld.net

Microsoft Revs Software Hosting

BY P.J. CONNOLLY

Although application service providers never took off the way they were supposed to during Bubble 1.0, the software-as-a-service model still recommends itself to customers large and small. Microsoft is making its own play for the SaaS dollar, with the recently introduced Windows-based Hosting Version 4.0, which was to become available worldwide on Aug. 4.

The new package includes support for SQL Server 2005 and ASP.NET 2.0, incorporating best practices and other guidelines gleaned from customer experiences since those products' release last fall.

According to Donovan Deakin, Microsoft's senior solution product manager in charge of Windows-based hosting, Microsoft is "seeing much more data-driven and dynamic Web sites out there that require scripting technologies."

Windows-based Hosting is one of three so-called "Solutions" that Microsoft offers service providers, with the company's hosted messaging and collaboration package and Windows-based Hosting for Applications. By the company's count, 142 service providers worldwide use Microsoft's Windows-based Hosting.

German Web host Intergetia services more than 2.2 million active sites on over 20,000 dedicated servers—making it the world's second-largest Web hosting provider, by Netcraft's reckoning—and almost all (more than 95 percent) of these sites run on Windows-based Hosting 3.5. ■



Enlightenment Through Virtualization

◀ continued from page 1

the companies are seeing eye-to-eye.

IBM, unlike Novell, views Xen as only one piece of a larger virtualization puzzle. Kevin Leahy, director of virtualization strategies at IBM, said that his company sees its role as providing overall management tools that can take care of multiple virtualization environments at once.

Sun, on the other hand, has been working with the Xen team to build up support for running Solaris under the virtualization platform, and HP has been contributing its minds to improving the platform.

Meanwhile, Microsoft announced that it plans to allow Xen to interoperate with its own hypervisor.

Jim Ni, group product manager of the Windows Server division at Microsoft, said that Longhorn will include a number of features that make virtualization a fundamental part of the operating system. "We're putting something we call Enlightenment in the core operating system, which allows the OS to understand it's virtualized. So Linux will run on top of Windows Server Longhorn."

Ni said that Microsoft's agreement with Xen Source will help to make Linux run more smoothly on Windows, and to allow Xen environments to transfer seamlessly to the new Windows virtualization platform. Ni also said that Microsoft will modify Windows to make it better able to run under Xen on other operating systems. "Windows does run on third-party virtual machine monitors. It runs on Xen Enterprise, and Microsoft is going to provide commercially reasonable efforts to support premier-level customers," said Ni, who refused to clarify what "commercially reasonable efforts" means.

RIVAL SPEAKS OUT

But that agreement isn't entirely to taste for rival virtualization company VMware. Raghu Raghuram, VMware's vice president of platform products, claimed that Microsoft is being disingenuous in its statements about the Xen Source agreement.

"This is a one-way arrangement where Microsoft will allow Linux to run on future Microsoft hypervisors through translated

calls to the hypervisor when Windows is controlling the hardware, but not the other way around. Under this arrangement, Longhorn Enlightenment will not be ported or

licensed to run on a Xen hypervisor," said Raghuram in a prepared statement. "It is notable that Microsoft's announcement is being made about a hypervisor whose first release is roughly

two years away or more, and while the Linux hypervisor interfaces are still being discussed in the community."

Raghuram went on to state that Xen is not nearly as mature

as his company's own virtualization platforms, which debuted in 2001.

Raghuram said that VMware's offerings are able to treat a pool of servers as a singular entity to be provisioned as needed, and that Xen does not yet offer the capabilities needed for large enterprise deployments. ■

Mindreef®
Quality and productivity
for the entire SOA lifecycle

Corporate Architect
Codify corporate standards, best practices, and governance policy around WSDL and schema

Project Architect
Leverage rules from corporate architects while creating shared workspaces that add documentation, example scripts, and simulation data to enhance the WSDL contract

Service Developer
Use shared workspaces from Project Architects to fully understand requirements. Create unit tests automatically during development

Client Developer
Enter the development process earlier with Mindreef's auto documentation and simulation features

Support Staff
Capture all associated problem artifacts into a Mindreef Shared Workspace*, allowing any team member to reproduce a problem at the push of a button

Testing
Leverage architect's example scripts and developer's unit tests to quickly and easily create robust regression tests

Mindreef SOAPscope®
Industry-leading Web services testing and diagnostics

Mindreef SOAPscope Server™
Design, develop, test, and support Web services as a team
NEW version 5.21

Mindreef's lifecycle approach—from well-adopted best practices early in the process to efficient problem resolution post-launch—drives down the cost of developing and maintaining Web services, leading to more efficient, higher-quality SOA. Mindreef products are designed to leverage your most valuable assets—your service team members—to achieve sustainable business results.

From your first Web service project to large SOA initiatives.
Download FREE trials at www.mindreef.com, or to speak with a Mindreef representative, call 603-465-2204 x581.

Mindreef®
QUALITY-DRIVEN SOA™

*patent pending
©2006 Mindreef, Inc. Mindreef and Mindreef SOAPscope are registered trademarks, and Mindreef SOAPscope Server is a trademark of Mindreef, Inc. in the United States and other countries. All rights reserved.

Wind River Linux Ready for Real Time

Focuses on handsets, carriers; contributes code to kick-start Eclipse projects

BY EDWARD J. CORREIA

Wind River Linux is ready for handsets. So says Wind River Systems, which unveiled its fourth Linux release on July 31, targeting ARM-based devices with a kernel footprint it claims comes in at less than 1MB.

"Wind River is now a viable, mature Linux company with a solid product line," asserted Glen Seiler, Wind River's senior manager for Linux platforms. Wind River Linux 1.3 is the first commercial implementation based on Linux kernel 2.6.14, released in October, the company claims.

Seiler said the latest kernel includes significant updates to the pre-emption patch developed by Ingo Molnar, and solves mutexes and other real-time performance-related issues. "We believe this is a better solution than prior kernels for aerospace and carrier grade customers [because of] its high-resolution timers and core performance-related functionality."

The platform also now includes enhancements to networking protocols and file systems, and increased hardware architecture support. It also is OSDL-certified compatible with its Carrier Grade 3.2 spec released in March, Seiler said. The updates are included in the Linux editions of Wind River's General Purpose Platform as well as its Consumer Devices and Network Equipment platforms, which also target x86 and PowerPC platforms.

Seiler said the distribution reduces the Linux footprint in large part by its use of uClibc, the C library for embedded systems that is smaller but mostly compatible with the GNU C library Glibc. Most applications written for Glibc require just a recompile. Wind River's distribution also now supports the BusyBox small-footprint Unix utility package and flash file systems. The entire distribution can be implemented on a device in about 4MB, he said.



'Wind River is now a viable, mature Linux company with a solid product line.'

—Glen Seiler, senior manager for Linux platforms

TOTAL ECLIPSE

Wind River also has made significant code contributions to the Eclipse Foundation—300,000 lines of code in all—that it says are designed to help speed up the C Development Tools (CDT) project as well as its own Device Software Development Platform (DSDP) project.

Among its DSDP contributions will be Terminal View, which will give Eclipse developers the ability to peer inside a

running device via serial connection from within the IDE. "For device developers, serial connectivity is one of the most common ways a developer gets debug information from a device," said Steven Heintz, Wind River's director of product management for developer tools. "Rather than going to an external program to see what's going on, this makes that a seamless experience," he said.

Wind River will also enhance the editor's code formatting symbol navigation capabilities, he said.

For the DSDP's device debugging project, the company is working on an extensible Eclipse debugging model—code-named Riverbed—to allow debugging views to coincide with the actual target architecture. "That's one of the key projects because an ARM 7 has fewer registers than an ARM 11. This will allow them to display the right number," Heintz said, for example.

To make that possible for the DSDP, Heintz said changes to Eclipse's core framework were required. Those changes were implemented with Callisto. "Wind River and other DSDP companies have had a positive impact on Callisto, laying the groundwork for plug-

gable debuggers and editors to exist. This will benefit not only device software developers but all C and C++ developers using Eclipse," he said.

Wind River also is working on creating pluggable parsers. Said Heintz: "The initiative is to break the parser from the editor so you can use the default parser in CDT or plug in a commercial parser," to allow parsers to be matched with languages. "There are different ways to do parsing for C and C++, and it's more difficult to do effective parsing for C than for, say, Java, which is strongly typed," he added. Wind River will contribute code from SNIFF+ parsing technology it acquired with ISI in 2001.

The DSDP's target management project also will get a boost, but more from IBM than Wind River. The two will work together to integrate the project with IBM's Remote System Explorer, which permits Eclipse to connect to remote Linux and Unix systems, see and edit files with Eclipse editors, and

compile and execute source code remotely. "We're contributing code in conjunction with that [to] make it more target-oriented so you can connect to and manage multiple targets," said Heintz.

Heintz said that projects under way now should reach completion by next year's joint release in June with regular milestone releases in the meantime. ■



'Serial connectivity is one of the most common ways a developer gets debug information from a device.'

—Steven Heintz, director of product management for developer tools

AppForge Customers Prompt Shift in Strategy

Company finds users want runtime for developing, deploying customer-facing apps

BY EDWARD J. CORREIA

About eight months ago, AppForge began to notice a shift in customer buying patterns. The company, which develops and markets a Visual Studio add-on for mobilizing enterprise applications, noticed that customers were suddenly buying more client licenses. A lot more. The company this month will reduce its volume pricing and adjust other licensing policies to reflect the new trend, it says.

"We went from selling about 1,000 licenses a month [total] to seeing deployments of 1,000 licenses a month from [individual] customers," said AppForge president Gary Warren. One customer, he said, was talking about purchasing 100,000 licenses a year.

After some analysis and group head-scratching, Warren said they realized that customers had begun to use Crossfire—the company's flagship runtime environment for targeting BlackBerry, Palm OS, Symbian and Windows Mobile—to develop and deploy customer-facing applications, a departure from typical enterprise deployments. "Customers had started using Crossfire not only for their line-of-business apps, but also to turn a Treo or BlackBerry into a Web services terminal."

Crossfire extends Visual Studio's drag-and-drop interface to allow targeting of mobile devices using .NET languages. Its native-like apps offer advantages over mobile browser-based apps for accessing Web-

based services, Warren claimed, because of the intermittency of wireless connections. "The mobile browser doesn't work," he said, claiming they are slow and hard to use. "You need software running on the device," he said. "There's no worries about phishing or other hacks because the client talks only to your site," he added, speaking of security.

Warren said that while the AppForge customer base now potentially includes banking, airline, medical services and other industries that develop customer-facing apps, its sales and marketing strategies will not change significantly. "It's more of an evolution, because the IT departments are still in charge of development. The

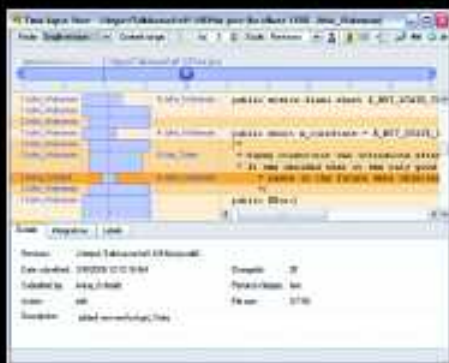
same people doing the baggage handling software are also doing the Web site," he said.

To address the change in customer buying patterns, AppForge later this month will officially unveil a new licensing policy that will adjust volume-based pricing and simplify application deployment with consumers in mind. The runtime will be included with the application. "End users don't want to know there's a runtime, and software companies don't want them to know," he said. Exact pricing was not set at press time.

The Crossfire runtime component runs natively on all devices except the BlackBerry, where it runs in a JVM due to carrier concerns. ■



Introducing Time-lapse View, a productivity feature of Perforce SCM.



Perforce Time-lapse View

Time-lapse View lets developers see every edit ever made to a file in a dynamic, annotated display. At long last, developers can quickly find answers to questions such as: 'Who wrote this code, and when?' and 'What content got changed, and why?'

Time-lapse View features a graphical timeline that visually recreates the evolution of a file, change by change, in one fluid display. Color gradations mark the aging of file contents, and the display's timeline can be configured to show changes by revision number, date, or changeset number.

Time-lapse View is just one of the many productivity tools that come with the Perforce SCM System.

Download a free copy of Perforce, no questions asked, from www.perforce.com. Free technical support is available throughout your evaluation.



ARE YOUR APPLICATIONS FEELING SECURE?

Network firewalls can't protect attacks through your applications. The first step toward proactive application security is to find and fix vulnerabilities.

Until now, manual testing, which is costly and time consuming, was your only option for securing web applications.

Now, you have a better option. CenZic's Software and Software as a Service (SaaS) Solutions deliver the accuracy of manual testing at a fraction of the cost and time.

FILL THE GAPS WITH CENZIC HAILSTORM® AND CENZIC CLICKTOSECURE™
The Most Intelligent Application Security Testing Solutions



For a free **IDC Vendor Spotlight** on the need for accurate web app testing, please go to <http://www.cenzic.com/sdtvs>

Please try one of our **free or eval products** at <http://www.cenzic.com/sdtfree>

Slipping In The Side Door With App Security Message

BY JENNIFER DEJONG



In the beginning, the strategy seemed obvious. Show development managers how the code their teams write can be compromised, and they will buy application security tools designed to help prevent the problem.

But, according to application security tool makers, things haven't turned out that way. Convincing development managers to adopt the source-code analyzers and black-box testing tools they sell has proved difficult, the tool makers acknowledged.

"It was naive to think developers would take up application security on their own," said Roger Thornton, founder and chief technology officer for Palo Alto, Calif.-based Fortify Software. They are already under a lot of pressure, he said. "Everyone is asking them for more features, faster."

Getting developers to adopt security tools is a tricky thing, added Mike Weider, founder and chief technology officer for Waltham, Mass.-based Watchfire. They are accustomed to writing code and handing it off to QA, he said. "They don't see testing as part of their role, and using the tools slows them down."

What's more, the popular sales tactic

of analyzing developers' code and identifying where and why the application is vulnerable to attack didn't exactly win developers over, noted Caleb Sima, founder and chief technology officer for Atlanta-based SPI Dynamics. "When you come along with a tool that shows developers what they did wrong, that's a frustrating experience," he said, which led many developers to rebel. "The developers said, 'I don't want you pointing out more problems for me. Just let me do my job.'"

GETTING THE MESSAGE

In spite of these hurdles, application security tools are making their way to developers' desktops, albeit by a more circuitous route.

Source-code analyzers, which scan code against a database of known vulnerabilities, and black-box testing offerings, which find security holes by attacking an application in much the same way a hacker might, are typically driven into development by the security professionals, according to the tool makers. Charged with carrying out mandates from top management, security professionals are setting policies that require development teams to adopt the tools, they said.

Until recently, security professionals were concerned largely with network-level security, which meant implementing firewalls and intrusion detection systems. But the importance of addressing security at the application level has made its way onto their radar screens, said Sima. "They know the firewall is not enough," he said. "The message has gotten through."

Now that companies recognize the problem, "we have moved beyond missionary selling," added Watchfire's Weider.

It is hard to say to what extent the tools are selling, as research firms have not estimated the size of the application security market alone. But an IDC report published in December 2005—"Worldwide Security and Vulnerability Management Software 2005–2009 Forecast and Analysis: Taking Control of the Security Environment"—projects that the overall security market, which also includes network security and security management tools, will grow to more than US\$3 billion by 2009. The report noted that software security vulnerability products geared to developers and QA professionals are growing in popularity.

Market projections aside, development teams are only just beginning to grasp the implications of building security into the application development process. "They are asking, 'How do I build application security into the fabric of my company?'" said Kevin Kernan, CEO for McClean, Va.-based Secure Software.

Given the cultural changes that adopting an application security strategy entails, the answer to that question is still evolving. But a few key things are clear, the tool makers said. To develop applications robust enough to withstand Web attacks, companies must address

security in every phase of development, beginning with requirements. Also essential is employing a dual approach that includes both white-box and black-box testing tools. Both offerings should be tied to the IDE in which the developer works, and they should strike a balance between offering enough information to be useful, but not so much that they slow developers down, said Nick Allen, director of marketing for Burlington, Mass.-based Klocwork. "You don't want to overwhelm developers with too much information." It's best to give them some latitude, letting them specify, for example: "Show me only the most critical vulnerabilities," he said.

WHITE BOX, BLACK BOX

Source-code analyzers, also known as white-box security tools, scan source code looking for well-known vulnerabilities that hackers could exploit with attacks such as SQL injections, or cross-site scripting errors. White-box tools let developers see the actual source code, said Secure Software's Kernan. "They walk you through it, showing you the tree structure behind the flaws you have discovered," he said. "Here's where the [vulnerability] originated; here's how to fix it."

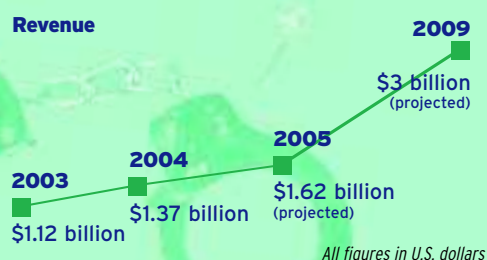
By contrast, black-box offerings, also known as penetration testing tools, offer no such window into the application. They simulate the behavior of a hacker in order to identify where the vulnerabilities lie. "They don't offer any contextual information," said Kernan. "You can't see the inside [the black box]."

But both approaches play a role, he said. White-box tools let developers analyze code as they work, while black-box tools are deployed during testing. "You want to be comprehensive and accu-

► continued on page 24

SPENDING FOR SECURITY

Products geared to testers and developers, such as source-code analyzers and black-box testing tools, are growing in popularity, IDC noted in its study. The overall market also includes security management and network security software.



Source: "Worldwide Security and Vulnerability Management Software 2005–2009 Forecast and Analysis: Taking Control of the Security Environment," IDC, December 2005

Slipping In App Security Message

◀ continued from page 23

rate,” added SPI Dynamics’ Sima. Combining the two technologies is the best way to do that, he said.

If secure coding efforts are to succeed, development managers need to start thinking about application security long before a line of code gets written. One meaningful way to do that is to create requirements use cases that specify “what you don’t want the system to do, not just what you want it to do,” said IBM Rational program director Ashok Reddy. For example, a use case could enable a buffer overflow, a commonplace programming error that can result in a security breach, he said.

IBM does not provide white-box or black-box security tools, but offerings from partners, including SPI Dynamics, and San Francisco-based Coverity, plug into the Rational Software Development Platform, said Reddy.

Focusing on security issues in requirements is key to helping development teams address security from the get-go and throughout the application life cycle, the tool makers said. That’s an

THE TOP 10 APPLICATION SECURITY THREATS

The Open Web Application Security Project (OWASP) is a not-for-profit foundation that provides guidelines to help organizations develop and maintain secure code. It monitors security threats and publishes the OWASP Top Ten, a list of the top vulnerabilities, which also provides remediation advice. Here is the current list.

Unvalidated input: Information from Web requests is not validated before it is used by a Web application, allowing attackers to exploit these flaws to attack back-end components through a Web application.

Broken access control: Restrictions on what authenticated users are allowed to do are not properly enforced. Attackers can exploit these flaws to access other users’ accounts, view sensitive files or perform unauthorized functions.

Broken authentication and session management: Account credentials and session tokens are not properly protected. Attackers that can compromise passwords, keys, session cookies or other

tokens can defeat authentication restrictions and assume other users’ identities.

Cross-site scripting: The Web application can be used as a mechanism to transport an attack to an end user’s browser. A successful attack can disclose the end user’s session token, attack the local machine or spoof content to fool the user.

Buffer overflow: Web application components in some languages that do not properly validate input can be crashed and, in some cases, used to take control of a process. Components can include CGI, libraries, drivers and Web application server components.

Injection flaws (such as SQL injections): Web applications pass parameters when they access external systems or the local operating system. If an attacker can embed malicious commands in these parameters, the external system may execute those commands on behalf of the Web application.

Improper error handling: Error conditions that occur during normal operation

are not handled properly. If attackers can cause errors that the Web application does not handle, they can gain detailed system information, deny service, cause security mechanisms to fail or crash the server.

Insecure storage: Web applications frequently use cryptographic functions to protect information and credentials. These functions and the code to integrate them have proven difficult to code properly, frequently resulting in weak protection.

Application denial of service: Attackers can consume Web application resources to a point where other legitimate users can no longer access or use the application. Attackers can also lock users out of their accounts or even cause the entire application to fail.

Insecure configuration management: Strong server configuration is critical to a secure Web application. These servers include many configuration options that affect security and are not secure out of the box.

Source: www.owasp.org

entirely new mindset for most companies, noted Watchfire’s Weider. “Security was something you [worried about] retroactively, after the fact.”

Even though development managers are responsible for addressing security

concerns throughout the application life cycle, they do not bear the burden alone, said Fortify’s Thornton. The work is done by development teams, but security professionals, who drove application security tool adoption in the first place,

are responsible for the final sign-off.

“I have looked at your code, and it’s fine. You are no longer accountable. I am,” said Thornton, assuming the role of the security professional. “For me, as a developer, that is how I would want it.” ■

VISUALIZE, DOCUMENT and CONTROL YOUR SOFTWARE PROJECT with ENTERPRISE ARCHITECT

From Concept to Solution – EA delivers team based UML® 2 modeling at an attractive price

Model with all 13 UML 2 Diagrams

Visualize using Industry-Standard Notation and Profiles

Collaborate Across All Roles in the Development Team

Integrate with Microsoft® Visual Studio® and Eclipse®

Support from 250+ Sparx VAR and Trainer Partners Globally



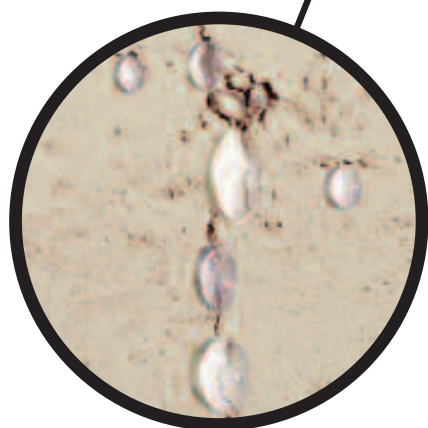
ENTERPRISE ARCHITECT

SPARX SYSTEMS

All product names are owned by their respective owners.

Download Your Free 30 Day Trial of Enterprise Architect at:
www.sparxsystems.com

THE SMALLEST SECURITY DEFECT COULD BE THE START OF A



BIG PROBLEM

Find Security Defects with QAInspect

QAInspect is a unique product that gives QA professionals the ability to incorporate automated Web application and Web services security testing into your test management process quickly and easily without impacting schedules or requiring security expertise.

- Extends existing functional tests with comprehensive security testing
- Includes testing and reports for more than 20 major laws, regulations and best practices
- Reports and prioritizes security defects alongside functional defects
- Seamlessly integrates with IBM Rational Software Development Platform (ClearQuest and Functional Tester)

FREE Trial Offer: Download a FREE trial and learn how QAInspect simplifies security for QA Professionals at www.spidynamics.com/QA.

Toll-Free: 1.866.774.2700

QAInspect is a trademark of SPI Dynamics.



EDITORIALS

Mercury's Uncertain Fate

Hewlett-Packard's purchase of Mercury Interactive may make good financial sense, and certainly helps HP better position its OpenView IT management business to compete against CA's UniCenter and IBM's Tivoli. However, given HP's size and focus on general IT, it does not bode well for software development and test/QA managers who rely upon Mercury's tools.

Mercury is a powerhouse in software performance management and testing. In the 2005 Testers Choice awards, a reader poll conducted by SD Times' sibling publication, Software Test & Performance, Mercury swept seven out of 14 categories with LoadRunner, TestDirector for Quality Center and QuickTest Professional.

When one company dominates software testing and performance management as thoroughly as Mercury, the prospect that the company will be subsumed into a behemoth with a US\$2.85 billion market cap and \$986 million in annual revenue is daunting—and frightening.

The most comparable acquisition in our space, that of Rational by IBM in early 2003, differed in that IBM was already a major player in software development. By contrast, while HP has a stellar reputation in IT management with OpenView, it's only peripherally been involved in software development and testing—and its previous experiences were lackluster at best.

The Mercury deal is also much bigger than the Rational purchase: HP is paying \$4.5 billion, nearly twice what IBM shelled out. The ripple effect that this purchase will have on the test market will likewise be huge.

Consider: Many Mercury test/QA customers may not want to become HP customers, especially if they don't use HP hardware, or if they prefer competing management platforms like Tivoli or UniCenter or Microsoft Operations Manager. Expect other test/performance companies to launch aggressive moves to migrate Mercury customers. While the lion's share might end up with the other giant, IBM Rational, there's a lot of room for players like Compuware, Empirix, Parasoft, Quest or Borland to pick up market share.

Also, the long-term fate of the Mercury test/performance products is unknown. Will HP aggressively invest in this new line of business? Will they sell the products off? Or will they be neglected and slowly die, just like Bluestone Software's middleware did after being purchased by HP in late 2000? This speculation may fuel additional acquisitions and investment in the test/performance space, as well as uncertainty.

Fuzz Testing: The Next Trick?

The Month of Browser Bugs, conducted by the Metasploit Project, was an interesting stunt. For the month of July 2006, H.D. Moore threw random data at popular Web browsers, and unearthed 27 security flaws, 23 of which were in Microsoft's Internet Explorer.

What does this say about Microsoft's software? Certainly many (but not all) of the high-profile security flaws lately have been found in Windows, Internet Explorer and Office. Because of their sheer market dominance, those products have long been targeted by worm and virus writers, as well as other black hats.

But fuzz testing, a respected but rarely discussed testing methodology, doesn't care about market dominance; it merely looks to see how well a piece of code handles random and malformed input. By that test, Microsoft did much worse than its competitors.

Was this a fair test? Yes. We don't have all the details about the MoBB project, but fuzzing is a valid way of testing security. After all, it's a technique that black hats can use as much as white hats. If you're vulnerable, you're vulnerable. And Microsoft software is vulnerable.

From the MoBB project, we can draw two conclusions. First, that more enterprise developers and ISVs should use fuzzing to test their own software. And second, that Microsoft still has plenty of room for improvement. ■

Forget Time-to-Market:
It's All About Time-to-Money

The popular business school metric time-to-market (TTM) is of little value to software development projects. And, even worse, it consistently offers incentives for counterproductive economic behavior. The problem is that time-to-market measures the ability of an organization to get a new product out the door whether or not that product will be successful in the marketplace.

A better way to measure performance would be to focus product efforts on time-to-money (TT\$), defined as the time it takes to deliver a product into the marketplace and achieve sustainable positive economic returns to its maker.

We've all participated in meetings where delivering a software product to meet a time-to-market goal was the metric tied to bonuses. Software developers know that any software train can arrive on time, if you don't care how many cars it has and if what were supposed to be Pullman sleepers turn out to be boxcars with faulty air brakes.

Users are smart. They keenly feel disappointment when software doesn't do what marketers promised, or behaves in unexpected and even dangerous ways. They tell their friends and clients. The sales pipeline dries up. And increasingly, wronged customers share their woes with product liability lawyers.

BILLIONS IN WASTE

Based on reports from the National Institute of Standards and Technology (NIST) and the Sustainable Computing Consortium, the total cost of software defects will reach an estimated US\$300 billion this year. This compares with an overall software investment of around \$600 billion. So, *half of every dollar spent on software goes down the tubes as cost-of-defects.*

But what if software development teams had to meet a different goal: time-to-money? Consider how the incentive structure would change if software teams were chartered to reduce the time between when product development begins and when products start to generate positive cash flow?

Products designed to shorten time-to-money would arrive to market with clearly differentiated features and benefits. They would delight customers and impress influencers. The product makers would face lower field support and return costs, and software suppliers would avoid the embarrassing, negative impact of poor quality on reputation and brand.

There's no doubt that a TT\$ incentive structure would change software develop-

ment practices. The current road to quality involves tedious, labor-intensive testing that has become synonymous with delay and expense. This is largely because software quality assurance is a back-ended process that involves torture-testing already-written code by trying it out in a variety of use cases until time runs out, and the product finally must ship.

Use cases range from the basic—"If I do what I'm supposed to, do I get expected results?"—to the exotic—"What happens to my application if I expose it to excessive cosmic rays?" (The author speaks from personal experience when it comes to cosmic ray testing.) In any event, the testers can't think of everything even if they had the time, and when it's all over, customers are expected to play their traditional role in completing the QA process.

ence when it comes to cosmic ray testing.) In any event, the testers can't think of everything even if they had the time, and when it's all over, customers are expected to play their traditional role in completing the QA process.

A BETTER WAY

Now if this were the process used in automotive or structural design, we'd have a lot more highway fatalities and structures collapsing. But these engineering disciplines have analytical tools that help them identify integrity issues before a car rolls onto the test track or a crew starts bulldozing for foundations. Electronic design automation for semiconductors provides an instructive example of how industrial-strength tools enable virtual design across teams with hundreds of developers placing and routing hundreds of millions of transistors onto substrates the size of a thumbnail. And these immensely complex products generally successfully announce "hello world" when first connected to power and signal sources.

These effective tools exist because of the economics associated with post-shipment quality issues for semiconductors. Time-to-money is severely impacted by defects, and since profitability is front-ended, delayed ramp to volume (caused by defective parts) can erase profit margins. Ironically, all of the heavy-duty engineering tools available to mechanical, electrical and structural engineers are written in software. Conversely, software developers are the cobbler's children who have no shoes.

But, can we really afford the cost of post-shipment software defects any longer? With today's applications numbering in the hundreds of thousands or millions of lines of code (and doubling every three years), and with defect densities ranging from one to 50 defects per 1,000 lines of code, we are sitting on a time bomb that ticks at a gigahertz pace.

So, after 45 years of Moore's Law, if



CPU cycles are all but free, where are the engineering tools to help developers create better software?

TOOLS TO USE

2004 and 2005 marked the first years of more widespread adoption of software structural analysis tools. Although light on engineering, these tools at least deal with basic hygiene issues, and can provide some level of assurance that coders aren't taking too many liberties and/or haven't succumbed to the management-prescribed "do more with less, but worse" practice that has characterized the post dot-com era.

But, these structural analysis tools alone won't guarantee software integrity. The industry needs analytical, engineering tools rooted in science and math (as opposed to process) that take advantage of plentiful, unused CPU cycles to assess software integrity across the development life cycle to deliver a continuous readiness assessment. Only a new generation of engineering tools can give development teams a fighting chance to deliver quality products. Software quality and time-to-money cannot improve significantly without them.

Time-to-money matters. In fact in most business, it's the leading indicator for success or failure. Borrowing what works from other advanced engineering disciplines would serve the software industry well. Beyond the technology, it has the potential to make each one of our daily lives better with respect to wealth, health and happiness. What's not to like? ■

Susan Kunz is president and co-founder of Solidware Technologies; before that, she worked at Sun Microsystems.

The Next Big Thing

The usual wisdom about programming-language lifetimes is that languages become obsolete just as they become mature enough to be standardized. Though Java has been standardized from day one, at 10 years old, it's starting to seem a little tired.

What's the next big thing, then? Certainly not C#, which is little more than a Microsoft-Certified Java with .NET libraries. And not scripting systems (I'm reluctant to call them languages) like PHP and Ruby, which are too Wild West to be trustworthy. No language that moves compile-time bugs into runtime is worth your time if you consider reliability to be important; I don't care how fast its adherents allege you can throw together a program. You don't measure productivity improvements solely by looking at a reduction in the lines-of-code-written-per-day numbers, even if these statistics are trustworthy.

While looking around the Web to see if something interesting is on the horizon, I stumbled across the Scala programming language (scala.epfl.ch), developed at the École Polytechnique Fédérale de Lausanne (EPFL) in Lausanne, Switzerland. A good overview of the language is at scala.epfl.ch/docu/files/ScalaOverview.pdf.

To quote the EPFL Web site: "Scala is a modern multi-paradigm programming language designed to express common programming patterns in a concise, elegant and type-safe way. It smoothly integrates features of object-oriented and

functional languages including mixins, algebraic datatypes with pattern matching, genericity and more [including operator overloading]. It is well integrated with Java and .NET: the Scala compiler produces standard Java class files or .NET assemblies, and Java/.NET libraries and frameworks can be used without glue code or additional declarations." It is a mature language, now at version 2.1.7.

The last bit of the earlier quote is particularly important. You can literally intermingle Java classes with Scala code without any work whatever. You can even do things like implement Java interfaces with Scala classes. This ability to integrate with existing libraries (which the Scala architects see as "components") is essential to any language that attempts to preempt Java.

The main strength of Java is its libraries, not the language itself. It's relatively easy to throw together a compiler, at least when you compare this effort with what's required to build the libraries that actually make the language useful.

In spite of all this wonderfulness (to quote Bill Cosby), I don't think Scala is a real candidate for the next big thing.

First, Scala has a hard-to-understand syntax, for a C++, C# or Java programmer. Java was largely successful because it was an easier-to-understand variant on a widely used language (C++). Scala's syntax is elegant from an academic perspective, but it's just too different from languages people already know to be widely accepted.

A more important question is whether another large general-purpose language is even a good idea. The more I program, the more fault I find in the accepted wisdom that it's good to build large systems in recursive layers that encapsulate the complexity of the underlying layer.

One way to look at Moore's Law is that every 18 months, we make machines fast enough to compensate for the inefficiencies we've added in the past 18 months.

The JVM provides a platform that lets you splice disparate languages and libraries together into a functional whole. That is, you can create a bunch of small tightly focused languages that do one thing (like build a UI) really well, and then create a system by melding together parts created in separate languages. This is nothing but Unix's hoary "small language" approach to programming, and it seems to work well in many applications.

Perhaps, then, the next big thing will actually be a lot of little things, working together to do a big job. ■

Java Watch



Allen Holub is an architect, consultant and instructor in C/C++, Java and OO Design. Reach him at www.holub.com.



Software Development Times
August 15, 2006 - Issue No. 156

Editor-in-Chief

David Rubinstein

+1-631-421-4158 x105

drubinstein@bzmedia.com

Executive Editor

Edward J. Correia

+1-631-421-4158 x100

ecorreia@bzmedia.com

Senior Editors

P. J. Connolly

pjconnolly@bzmedia.com

Jennifer deJong

jdejong@bzmedia.com

Alex Handy

+1-510-282-4840

ahandy@bzmedia.com

Editorial Director

Alan Zeichick

+1-650-359-4763

alan@bzmedia.com

Columnists

Andrew Binstock

Allen Holub

Larry O'Brien

Managing Editor

Patricia Sarica

psarica@bzmedia.com

Art Director

Mara Leonardi

mleonardi@bzmedia.com

Art/Production Assistant

Erin Broadhurst

ebroadhurst@bzmedia.com

Contributing Writers

Geoff Koch

Susan Messenheimer

Lisa L. Morgan

Carol Weiszmann

Special Projects Editor

George Walsh

gwalsh@bzmedia.com

Publisher

Ted Bahr

+1-631-421-4158 x101

ted@bzmedia.com

Associate Publisher

Charlie Shively

+1-508-893-07364

cshively@bzmedia.com

Advertising Sales

Southwest U.S./Asia

Robin Nakamura

+1-408-445-8154

rnakamura@bzmedia.com

Southeast U.S./Europe

Jonathan Sawyer

+1-603-924-4489

jsawyer@bzmedia.com

Northwest U.S./Canada

Paula F. Miller

+1-925-831-3803

pmiller@bzmedia.com

Northeast/North Central U.S./Canada

David Lyman

+1-978-465-2351

dlyman@bzmedia.com

Advertising Traffic Manager

Phyllis Oakes

+1-631-421-4158 x115

poakes@bzmedia.com

Director of Circulation

Agnes Vanek

+1-631-421-4158 x111

avanek@bzmedia.com

Circulation Assistant

Nyla Moshlak

+1-631-421-4158 x124

nmoshlak@bzmedia.com

Director of Editorial Operations

David Rubinstein

+1-631-421-4158 x105

drubinstein@bzmedia.com

Director of Events

Donna Esposito

+1-415-785-3419

desposito@bzmedia.com

Controller

Viena Isaray

visaray@bzmedia.com

Office Manager/Marketing

Cathy Zimmermann

+1-631-421-4158 x108

czimmermann@bzmedia.com

Web Developer

Craig Reino

creino@bzmedia.com

Web/HTML Producer

Nicole Schnatz

nschnatz@bzmedia.com

Article Reprints

Lisa Abelson

Lisa Abelson & Co.

+1-516-379-7097

labelson@bzmedia.com

Customer Service/Subscriptions

+1-847-763-9692

sdtimes@halldata.com

Do You Get the Most From Your Enterprise Apps?

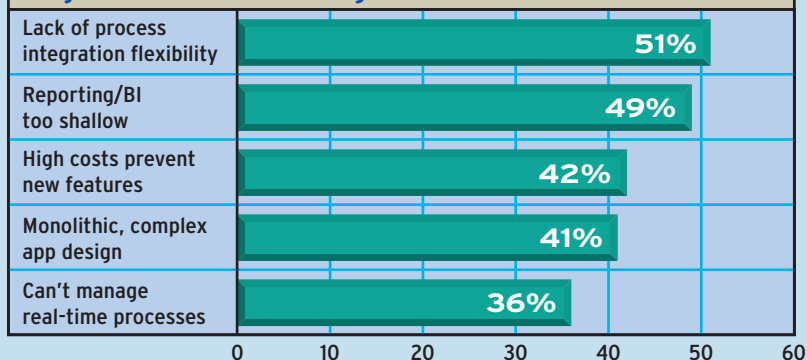
DATA WATCH

An Aberdeen Group study published in May found that workers are losing a significant amount of productivity due to improper or absent integration between enterprise applications, which it deems essential to maximum efficiency.

The benchmark report, titled "Achieving More Value From Enterprise Applications," estimates that companies stand to save a combined US\$143 billion in 2006 if they were to adopt best-in-class software maintenance and cost-efficiency practices, such as proper application selection and integration through SOA enablement.

For the study, Aberdeen Group polled a varied range of executives and IT staff from a mixture of large, midsize and small companies, mainly in the U.S. and Europe.

Major Roadblocks to Integration



Allen Holub is an architect, consultant and instructor in C/C++, Java and OO Design. Reach him at www.holub.com.

BZ Media



President

Ted Bahr

Executive Vice President

Alan Zeichick

BZ Media LLC

7 High Street, Suite 407

Huntington, NY 11743

+1-631-421-4158 • fax +1-631-421-4045

www.bzmedia.com • info@bzmedia.com

Java EE Arrives. Then, the Big Yawn

For years, I have been carrying on about the complexity of writing Java enterprise apps. My complaints fall into two broad categories: the pain of using Java as an application language, and the difficulty of mastering the constituent technologies of J2EE, the former enterprise Java framework.

There is a third aspect of complexity that I won't go on about, but which must be faced by most developers: the plethora of add-on technologies and Java frameworks (XML, Web services, JSPs, Struts, JavaServer Faces, Spring, Beehive, Hibernate and so on.) You don't need them all, but you do need to know some subset to write enterprise Java apps.

Returning to the language and the J2EE platform, we finally got substantial relief this year in the Java EE release. It definitely reduces the complexity of enterprise apps by simplifying the use of EJBs and providing more straightforward persistence mechanisms. It also makes extensive use of annotations (which are a set of concise statements that specify the role played by chunks of code. Annotations were first introduced into the Java language in the Java 5 release.)

With all this goodness delivered after a prolonged and vocal demand for reduced complexity, you would think the commu-

nity would be jumping for joy and celebrating this new release, right? Nothing doing. At the JavaOne developer love-in this year, Java EE was covered but not feted. And, to put it mildly, this year's show was one that cried out for some kind of announcement to focus on. It could have been the "Java EE show," but even Sun, it appeared, was yawning at the new release.

What gives? Richard Monson-Haefel, now an analyst for Burton Group but previously a member of the JCP expert group for EJB 2.1 and 3.0 and a co-founder of the Apache Geronimo project, writes that the new version "has failed to make Java EE less complicated. JEE 5's failure to address complexity is a harbinger of the Java EE platforms' fall from dominance in the enterprise development platform arena. Organizations should look elsewhere when considering new enterprise development and should plan for the eventual sunset of Java EE as an enterprise solution." Strong words, and not altogether correct, in my view.

First of all, I should note that this report came out at the same time as the most recent edition of Monson-Haefel's

own book on EJBs, the excellent "Enterprise JavaBeans 3.0" from O'Reilly and Associates, co-authored with Bill Burke. (To be fair, Burke did most of the work—essentially updating Monson-Haefel's earlier edition to cover EJB 3.0.) In it, Monson-Haefel touts the benefits of the new standard "that greatly simplifies the

Integration Watch



EJB programming model." In his report for Burton Group, however, he contends that Microsoft .NET (especially), open-source Java frameworks and Ruby on Rails are the new models that will eventually squeeze out Java EE.

His view is shared by many others, especially those who have already embraced those solutions. But I don't believe it. Microsoft .NET is certainly a challenger to enterprise Java. However, it has yet to make the deep penetration into large-scale enterprise situations, although it is moving in that direction. Its benefits (one company, one set of integrated solutions) are offset by Microsoft's long track record as an unreliable partner for enterprises. (Consider the forced technology transitions, the poor track record of product delivery, and the ongoing inability to create host operating systems that don't

require regular reboots. Only once these aspects are solved will Microsoft have enterprise creds.)

The open-source frameworks are a different story. They do simplify many tasks, but they lack the complete set of enterprise features. They surely make sense in the SMB space and in enterprises with modest needs. However, for them to take over larger computing centers from Java EE, they will need to add many new features and services—resulting in a corresponding increase in complexity.

Ruby on Rails (RoR) has truly ingenious design decisions that make rapid development of large projects possible. However, it is not currently capable of enterprise-scale workloads. The primary reason for this is performance. It is far slower than Java, and lacks testing in high-volume contexts. Finally, it's not clear that RoR provides all the necessary services in an integrated, enterprise-scale package. Adding these services will add complexity. How RoR handles this challenge will determine its role and its longevity, but for now, it's not a competitor to Java EE.

I think Java EE has legs. It drives many of today's largest sites and will continue to do so for a long time. Plus, it's not standing still. Refinements and simplifications will continue to be made, leading to a deployment life far longer than naysayers expect. ■

Andrew Binstock is the principal analyst at Pacific Data Works.

The Art & Science of Software Testing

A Special Supplement to SD Times

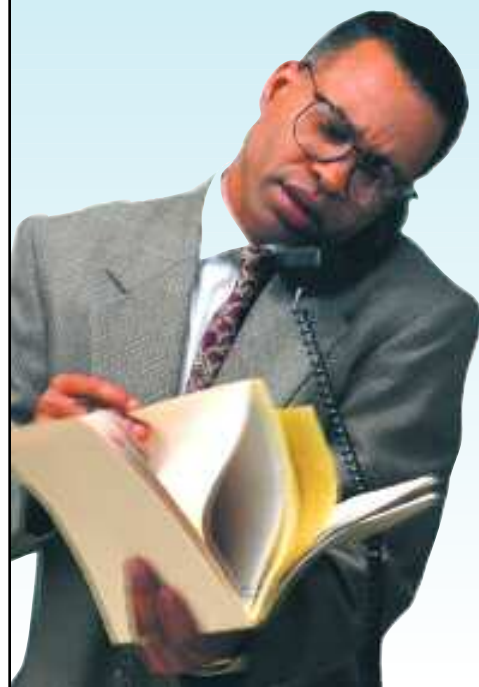
"The Art & Science of Software Testing" will highlight the leading tools and solutions for software testing and quality assurance, including:

- Application Life-Cycle Management
- Build Management
- Change/Configuration Management
- Debuggers
- Defect Trackers
- Embedded & Mobile Test Solutions
- Performance Management/Optimization
- Requirements Management
- Security Analysis Tools
- Security Testing Suites
- Test Automation
- Testing Services
- Vulnerability Testing Tools
- Web Load Testing
- Web Security Testing
- Web Services/SOA Testing



"The Art & Science of Software Testing" is brought to you by BZ Media, publisher of SD Times, the industry's most trusted source of software development news and analysis.

Look for it with the October 1 issue!



New Looks at Books

Physical books will always be important to a professional programmer.

Everything from the resolution (no one clamors for more than 15 diagonal inches in a book!) to the tactile aesthetics of high-grade paper, as well as the superb portability and relative ruggedness, weighs in on the value of print. On the other hand, books are heavy and they take up shelf space.

What's more, it's difficult to spend \$65 to access five pages on some API that you'll likely never use again, especially when you don't have the shelf space to keep the book on the off chance that it contains some other five pages that would apply in some other project down the line.

For those situations, online reference libraries like Safari and Books24x7 promise a solution. Both allow you to access a large library of works from a number of different publishers, read them online, and download a specific chapter for individual use. In both, browser-based reading is done in a single HTML-based column with a tree control on the left allowing access to other chapters, index and so forth. Both have tools for annotations and bookmarks. Safari is in the process of rolling out interface upgrades that significantly increase the amount of text returned per HTML page

(a noticeable improvement) and that allow delivery of "graphically rich" books like the "Head Start" series (a less successful experiment involving bitmapped images of the pages). A seemingly similar service is the utterly unworthy Amazon digital library, which gives you online access to a digital version of a book you've bought in print. The digital version is a bitmapped scan of the page, complete with background noise, and it's unthinkable to imagine paying for the privilege of reading a complete chapter, much less a complete book, in such a way.

I compared the two services in two areas in which many books have been published over the years: artificial intelligence and C++.

In AI, the results were unequivocal: Safari's eight selections included several that weren't really AI-related ("Voice Application Development With VoiceXML"), and the three books with "AI" in the title were all for game programming. Books24x7, in contrast, returned 31 results, including works from the presses of MIT, Cambridge University and Morgan Kaufmann. Books24x7's relationship with academic

publishers seems to give the service better depth than Safari, and not just in esoteric subjects—the immensely pragmatic Scott Ambler, for instance, publishes with Cambridge University Press.

In C++, the results were more ambiguous. Both had similar quantities (65 books in Safari, 88 in Books24x7).

Windows & .NET Watch



Larry O'Brien

Safari emphasized titles by O'Reilly (naturally) and Addison-Wesley, while Books24x7 had a significantly broader array of publishers, with perhaps an emphasis on Wiley, APress and McGraw-Hill/Osborne. Titles from Course Technology, Microsoft, Premier, Press, Que and Sams were found on both. Despite Books24x7's slight numerical edge, the Addison-Wesley Professional imprimatur is the best for C++, so I give the nod to Safari on that account.

However, neither service provides any of Bjarne Stroustrup's books! This is a telling shortcoming, which is that these services are not true reference libraries, but simply catalogs of books that pass some gamut of licensing and binary availability. This is obvious when "The C++ Programming Language" is not available, but is also true in the AI returns, where

the high quality of some Books24x7 returns (including "the" book on support vector machines) might disguise the holes in other areas (say, evolutionary computation). In this way, these online services remind me less of a library and more of a used-book store: You might find a gem, but because you can't rely on finding even a pretty good book on a given subject, it's hard to rely on them as the front line of your reference library.

Safari starts at US\$10 per month for access to five books per month. Access to a book is limited until you "put it on your bookshelf," and thus bite into your monthly allocation. In my experience, a "5-slot" bookshelf is just too limiting; a 10-slot bookshelf with the ability to download five PDF chapters per month is \$20.

Books24x7 requires a bigger commitment: Access to the "ITPro" collection costs US\$495 per individual per year. Corporate licenses are available, and Books24x7 seems to emphasize the corporate channel: In addition to the high immediate cost, it has the ability to assemble "corporate libraries" of titles, etc. These prices would be one thing if the services had comprehensive coverage. To me, these services are priced a shade too high. I guess I'll have to buy more shelves for the garage. ■

Larry O'Brien is a technology consultant, analyst and writer. Read his blog at www.knowing.net.

Instantly Search Terabytes of Text



- ◆ over two dozen indexed, unindexed, fielded data and full-text search options
- ◆ highlights hits in HTML, XML and PDF, while displaying links, formatting and images
- ◆ converts other file types (word processor, database, spreadsheet, email and attachments, ZIP, Unicode, etc.) to HTML for display with highlighted hits
- ◆ Spider supports static and dynamic Web content, with WYSWYG hit-highlighting
- ◆ API supports .NET/.NET 2.0, C++, Java, SQL databases. New .NET/.NET 2.0 Spider API

dtSearch® Reviews

- ◆ "Bottom line: dtSearch manages a terabyte of text in a single index and returns results in less than a second" — *InfoWorld*
- ◆ "For combing through large amounts of data, dtSearch 'leads the market'" — *Network Computing*
- ◆ "Blindingly fast" — *Computer Forensics: Incident Response Essentials*
- ◆ "Covers all data sources ... powerful Web-based engines" — *eWEEK*
- ◆ "Searches at blazing speeds" — *Computer Reseller News Test Center*
- ◆ "The most powerful document search tool on the market" — *Wired Magazine*

For hundreds more reviews — and developer case studies — see www.dtsearch.com

Contact dtSearch for fully-functional evaluations

The Smart Choice for Text Retrieval® since 1991

1-800-IT-FINDS • www.dtsearch.com

.NET Imaging

soars



Optimized for
Microsoft
Visual Studio .NET

Document Imaging Takes to the Air.

Using Atalasoft Imaging Toolkits your business can create applications that save time and money. Our .NET imaging components are designed exclusively for the Microsoft .NET Framework, offering developers Photographic and Document imaging for web and windows based applications featuring AJAX-enabled web imaging, PDF support, data capture, scanning/OCR, barcode reading systems, image management, and archiving just to name a few.

Fast and Dependable Imaging for .NET

www.atalasoft.com

toll free 866-568-0129

A 12-Step Program

The debate over what to do with substance abusers rages on. Throw 'em all in jail, many argue, to keep our streets safe from the crimes they commit to support their addiction. Rehabilitate them, others argue, so their behavior will change and they no longer will be a menace to society.

So, what to do with Microsoft, the Robert Downey Jr. of the technology industry?

The company has been fined millions of dollars and paid out multimillions more to settle lawsuits based on what several courts have called the company's monopolistic business practices. Those were the crimes Microsoft committed to acquire more substance—in this case, deals to lock others out of the browser, operating system and office productivity software markets so Microsoft could achieve dominance there and rake in billions of dollars in revenues. This company has a serious cash jones.

But suddenly, on the heels of the latest European Union action to fine Microsoft for failing to correct its business practices, the company declared it wants to be rehabilitated. It even went so far as to spell out the 12-step program it will undergo to become a better corporate citizen and no longer be a menace to competing software companies everywhere.

In a story that one would have thought would have been more widely covered if for nothing more than sheer entertainment value—and because the announcement was made at the National Press Club in Washington, D.C.—Microsoft general counsel Brad Smith laid out 12 voluntary tenets that he said the company will follow from here on in regarding the development

of the Windows desktop platform. (See them at www.microsoft.com/presspass/newsroom/winxp/windowsprinciples.mspx)

Believable? You decide. To me, it has the credibility of Downey Jr. himself, after leaving rehab for the umpteenth time, declaring that this time he has seen the error of his ways and from here on out will be clean and sober.

Industry Watch



David Rubinstein

But you've got to hand it to Microsoft. At least Smith put those principles out there, even if they're met with heaping piles of skepticism bordering on mockery. After all, Downey went into rehab pretty much after each of his arrests, and the jury's still out—pardon the expression—on whether or not he's a changed man.

Before seeing the light, the first commandment under which Microsoft operated was "Thou Shalt Have No Other Operating Systems Before Me." Now, Smith said the five tenets beneath the first principle, "Choice for Computer Manufacturers and Customers," call for the company to make it easier to install non-Microsoft programs instead of or in addition to Windows features, such as Windows Media Player and Internet Explorer. "Ultimately," and I quote the explanation given on the Microsoft Web site, "end users are free to choose which software they prefer to use."

How wonderfully generous of them! John Lennon, were he still alive, would be so moved as to write a song about this revelation... "Imagine there's no lock-in. It isn't hard to do..."

Under the second principle, called "Opportunities for Developers," Microsoft says it won't block access to any lawful Web site or impose a fee for reaching a non-Microsoft Web site or Web service. It will provide APIs that

let competing products plug into Windows as easily (or poorly, some might say) as Microsoft's own. It will separate out Windows Live, the Internet services piece, from Windows. Last, it lets developers know they are free to develop products that compete with any part of Windows, without any retaliation from Microsoft.

Under the final heading of "Interoperability for Users," we are left with the knowledge that Microsoft will support a range of industry standards in Windows, license its patents under fair and reasonable terms, and make available "on commercially reasonable terms" all the communications protocols it has built into Windows.

It seems to me an earlier set of guiding principles—written thousands of years ago—spelled out many of these same behaviors: Get along with others, don't covet your neighbor's software inventions, don't kill off competing companies.

Maybe Microsoft's executives have seen the light. Maybe they realize that as Linux and open source finally grow into viable alternatives, an all-or-nothing strategy would be a losing one in the long term. Maybe Bill Gates' humanitarian streak has begun to trickle down through the company.

And maybe, like a common drunk who's temporarily back on the wagon, it's putting on a brave face and stout demeanor to prove it can change. I can think of nothing that would benefit our industry more than Microsoft making its platform truly interoperable with other systems and software.

But I'm not convinced. That cash jones can be a powerful thing. Let's see how the company behaves when all this sharing and good-neighbor stuff results in declining revenues, and the Redmond bigs find themselves forced to go cold turkey on money. Will that drive them back to the drink? It's a slippery slope. ■

David Rubinstein is editor-in-chief of SD Times.

BUSINESS BRIEFS

Enterprise Java company **Terracotta** has named Amit Pandey CEO to help grow out the company's clustered JVM technology. Before joining Terracotta, Pandey held VP positions at Network Appliance. Terracotta founder and CTO Ari Zilka wants Pandey to continue driving Terracotta into the financial services, retail, telco and Internet services markets, where the technology is experiencing an uptake, according to the company. "Terracotta is drop-in technology that is easy to deploy and makes all Java applications enterprise-class," Pandey said. "Our technology has industry-shifting ramifications because it requires no coding. We make open-source software enterprise-ready, so it's a viable alternative to many commercial solutions." Terracotta's ability to bring caching and clustering into the Java runtime environment adds fault tolerance, scalability and high availability to any Java application, the company said.

EARNINGS: Microsoft announced record fourth-quarter revenue of US\$11.8 billion, a 16 percent increase over the same year-ago quarter. Net income for the quarter ended June 30 was \$2.83 billion, or 28 cents per

share, down from the same period a year earlier when the company posted net income of \$3.70 billion and EPS of 34 cents. For the fiscal year, Microsoft had revenue of \$44.28 billion, up 11 percent from the previous year. Net income for the year was \$12.60 billion. The company also announced a share repurchase program of \$20 billion to be completed by Aug. 17, and authorized an additional \$20 billion buyback with an expiration date of June 30, 2011. . . . **Compuware** reported fiscal 2007 first-quarter revenue of US\$296.3 million and net income of \$29.3 million, up from net income of \$24.6 million in the same quarter of fiscal 2006. Professional services accounted for \$118.5 million in revenue, while maintenance fees were \$110.3 million and software license fees were \$67.5 million. . . . **Informatica** reported revenue of US\$80.8 million, up 26 percent from the year-earlier quarter, and net income of \$7.6 million for its fiscal 2006 second quarter. . . . Performance management solutions provider **Applix** reported fiscal second-quarter 2006 revenue of US\$13.32 million, a 41 percent increase over the \$9.43 million posted in the same year-ago quarter. ■



CALENDAR OF EVENTS

EclipseWorld 2006 Boston BZ MEDIA www.eclipseworld.net	Sept. 6-8
VSLive New York City FAWCETTE TECHNICAL PUBLICATIONS www.ftponline.com/conferences/vslive/2006/newyork	Sept. 10-13
SD Best Practices Conference Boston CMP MEDIA www.sdexpo.com/2006/sdbp	Sept. 11-14
High Performance on Wall Street New York City LIGHTHOUSE PARTNERS & FLAGG MANAGEMENT www.highperformanceonwallstreet.com	Sept. 18
Application Development Summit Phoenix GARTNER www.gartner.com/2_events/conferences/ad8.jsp	Sept. 25-27
Embedded Systems Conference Boston Boston CMP MEDIA www.embedded.com/esc/boston	Sept. 25-28
Intel Developer Forum San Francisco INTEL www.intel.com/idf	Sept. 26-28
Open Source Summit Phoenix GARTNER www.gartner.com/2_events/conferences/os2.jsp	Sept. 27-29
Symposium/ITxpo Orlando, Fla. GARTNER www.gartner.com/it/sym/2006/_sym16/sym16_home.jsp	Oct. 8-13
Mercury World Las Vegas MERCURY INTERACTIVE www.mercuryevents.net/mercuryworld/home.cfm	Oct. 8-11
STAR West Anaheim SOFTWARE QUALITY ENGINEERING www.sqe.com/starwest	Oct. 16-20
SoftSummit Santa Clara MACROVISION www.softsummit.com	Oct. 17-18
Development Products Conference San Jose EVANS DATA www.evansdata.com/dpc	Oct. 19-20
Oracle OpenWorld San Francisco ORACLE www.oracle.com/openworld	Oct. 22-26
OOPSLA Portland, Ore. ACM SIGPLAN www.oopsla.org/2006	Oct. 22-26
Software Test & Performance Conference Boston BZ MEDIA www.stpcon.com	Nov. 7-9

For a more complete calendar of U.S. software development events, see www.bzmedia.com/calendar. Information is subject to change. Send news about upcoming events to events@bzmedia.com.

Automated Build Studio

simplify your deployment

Automated Build Studio is the perfect tool for building and releasing our software and it makes my working day so much easier.

Bart Roozendaal
SEVENSTEPS

SIMPLIFY BUILD PROCESSES
Eliminate manual operations and complicated scripts

VISUAL MACRO CREATION
Just drag and drop operations and set parameters

POPULAR TOOLS SUPPORT
Built-in support for more than 400 build and deploy operations

DETAILED REPORTS
Executive overview and detailed logs via the desktop client or web browser

CONTINUOUS INTEGRATION
Automatically build and test with every check-in

VISUAL STUDIO INTEGRATION
Run stand-alone or integrated with Microsoft Visual Studio

ONLINE ALERTS
Notify developers, testers and managers with instant messaging, email, text/sms

CUSTOM OPERATIONS
Easily create new operations with the comprehensive SDK

REMOTE WEB INTERFACE
Launch and monitor builds securely from any web browser

Automated Build Studio is a release management system that provides an easy and visual way to automate the software development build and deployment process. Create visual macros with drag and drop pre-built operations. More than 400 built-in operations are included for most popular tools.

\$349.99

Named user license
Concurrent & site licenses available

- 60 Day Money Back Guarantee
- Unlimited Online Support
- Free Evaluation



DOWNLOAD A FREE TRIAL
www.automatedqa.com/abs/sdoffer/

AutomatedQA
test, debug, deliver!

702-891-9424



_INFRASTRUCTURE LOG

_DAY 15: This project is out of control. The development team's trying to write apps supporting a service oriented architecture...but it's taking FOREVER!

_DAY 16: Gil has resorted to giving the team coffee IVs. Now they're on java while using JAVA. Oh, the irony.

_DAY 18: I've found a better way: IBM Rational. It's a modular software development platform based on Eclipse that helps the team model, assemble, deploy and manage SOA projects. The whole process is simpler, faster and all our apps are flexible and reusable. :)

_The team says it's nice to taste coffee again, but drinking it is sooo inefficient!



Rational.

Download the IBM Software Architect Kit at:
IBM.COM/TAKEBACKCONTROL/FLEXIBLE